

$\mathfrak{M}_H(G)$ -property and congruence of Galois representations

Meng Fai Lim*

Abstract

In this paper, we study the Selmer groups of two congruent Galois representations over an admissible p -adic Lie extension. We will show that under appropriate congruence condition, if the dual Selmer group of one satisfies the $\mathfrak{M}_H(G)$ -property, so will the other. In the event that the $\mathfrak{M}_H(G)$ -property holds, and assuming certain further hypothesis on the decomposition of primes in the p -adic Lie extension, we compare the ranks of the π -free quotient of the two dual Selmer groups. We then apply our results to compare the characteristic elements attached to the Selmer groups. We also study the variation of the ranks of the π -free quotient of the dual Selmer groups of specialization of a big Galois representation. We emphasize that our results *do not* assume the vanishing of the μ -invariant.

Keywords and Phrases: Selmer groups, admissible p -adic Lie extensions, $\mathfrak{M}_H(G)$ -property, π -free quotient.

Mathematics Subject Classification 2010: 11R23, 11R34, 11F80, 16S34.

1 Introduction

Throughout the paper, p will always denote a rational prime. Let \mathcal{O} be the ring of integers of a fixed finite extension K of \mathbb{Q}_p , and fix a choice of a local parameter π of \mathcal{O} . Let F be a number field and F_∞ an admissible p -adic Lie extension of F with Galois group G . For a Galois representation defined over a number field F with coefficients in \mathcal{O} , one can attach a Selmer group to these data and this Selmer group carries a natural module structure over the Iwasawa algebra $\mathcal{O}[[G]]$. The main conjecture of Iwasawa theory is then a conjecture on a precise relation between the Selmer group and a conjectural p -adic L -function (for instance, see [5, 6, 8, 13, 14, 16, 17, 25, 37]). In this paper, we are interested in comparing the Selmer groups of two congruent Galois representations. One of the motivations behind this study lies in the philosophy that the “Iwasawa main conjecture” should be preserved by congruences. Therefore, in view of this philosophy, one expects that the various Iwasawa theoretical invariants of the Selmer groups of two congruent Galois representations should be related. Over the cyclotomic \mathbb{Z}_p -extension, such studies were carried out in [1, 4, 13, 17, 18, 19, 37, 46]. Over a noncommutative p -adic Lie extension, this has also been carried out in [5, 7, 11, 24, 30, 32, 40, 41, 42] to some extent.

In the situation of a cyclotomic \mathbb{Z}_p -extension, Greenberg and Vatsal first considered the situation of two elliptic curves with good ordinary reduction at the prime p , whose p -torsion points are isomorphic

*School of Mathematics and Statistics & Hubei Key Laboratory of Mathematical Sciences, Central China Normal University, Wuhan, 430079, P. R. China. E-mail: limmf@mail.ccnu.edu.cn

as Galois modules. They proved that if the μ -invariant of one vanishes, so will the other, and they also compared the λ -invariants of the Selmer groups (see [18, Theorem 1.4]). Following their footsteps, Emerton, Pollack and Weston established similar results for Selmer groups of the specializations of a Hida family (see [18, Theorems 1 and 2]). Since then, many authors have obtained similar results for more general Galois representations (see [46, Theorems 1, 2] and [19, Theorem 1.1]). In the situation of a noncommutative p -adic Lie extension, analogous results have been obtained, and to describe these results, we need to introduce some more terminology. A Galois extension F_∞ of F is said to be an *admissible p -adic Lie extension* of F if (i) $G = \text{Gal}(F_\infty/F)$ is compact p -adic Lie group, (ii) F_∞ contains the cyclotomic \mathbb{Z}_p extension F_{cyc} of F and (iii) F_∞ is unramified outside a finite set of primes. Write $H = \text{Gal}(F_\infty/F_{\text{cyc}})$. In [5, Corollary 4.4.2], [7, Theorems 4.2 and 4.11], [24, Proposition 15], [30, Proposition 5.3] and [41, Theorem 8.4], it is proved that for two congruent Galois representations, if one of the dual Selmer groups is finitely generated over $\mathcal{O}[[H]]$, so is the other. Furthermore, they have also established relationship between the $\mathcal{O}[[H]]$ -ranks of two dual Selmer groups. A common feature in all the above cited works is that it is shown that whenever the Iwasawa μ -invariant of one of the Selmer groups vanishes, so does the other. It is then natural to consider the situation when the said Iwasawa μ -invariants are nonzero. In this situation, it is convenient to divide the problem into two, namely comparing the π -primary submodules of the dual Selmer groups and comparing the π -free quotient of the dual Selmer groups. For the comparison of the π -primary submodules of the dual Selmer groups, the first attempt to make such a study was done by Barman and A. Saikia (see [4]), where they compare the μ -invariants of the Selmer groups of two congruent elliptic curves over the cyclotomic \mathbb{Z}_p -extension. This result was later extended to more general Galois representation over a noncommutative admissible p -adic Lie extension in [5, 32]. It is worthwhile mentioning that the results of the author in [32] proves a finer statement, namely, the π -primary submodules of the dual Selmer groups of congruent Galois representations have the same elementary representations (see [32, Theorem 4.2.1]). For the comparison of the π -free quotient of the dual Selmer groups, this was first considered by Ahmed and Shekhar for two congruent elliptic curves over the cyclotomic \mathbb{Z}_p -extension (see [1, Theorem 3.1]). In this paper, we will consider the comparison of the π -free quotient of the dual Selmer groups of an admissible p -adic Lie extension (and for more general Galois representations).

We now like to mention the following. For two congruent Galois representations, one may ask if one of the dual Selmer group is a torsion $\mathcal{O}[[G]]$ -module, is the other one also torsion? In the context of [1, 7, 13, 18, 24], this is not an issue, as they already have the torsionness of Selmer groups by the results of Kato [26]. In all previous works (for instance, [19, 30, 41, 46]), the preservation of torsionness is established under the stronger hypothesis that one of the dual Selmer group is a finitely generated $\mathcal{O}[[H]]$ -module. The preservation of torsion property under congruence (of a high enough power) has only been recently obtained by the author in [32, Theorem 4.2.1]. In this paper, we like to go one step further, namely, we like to establish the preservation of the so-called $\mathfrak{M}_H(G)$ -property under congruence. In particular, in view of the discussion in the previous paragraph, this paper can be thought as a complement to the results in [32], and at the same time, an extension of the results there.

A finitely generated $\mathcal{O}[[G]]$ -module M is said to satisfy the $\mathfrak{M}_H(G)$ -property if its π -free quotient $M_f := M/M(\pi)$ is finitely generated over $\mathcal{O}[[H]]$. Here $M(\pi)$ denotes the π -primary submodule of M . It has been conjectured for Galois representations coming from abelian varieties with good ordinary reduction at p or cuspidal eigenforms with good ordinary reduction at p , the dual Selmer group associated to such a Galois representation satisfies the $\mathfrak{M}_H(G)$ -property (see [8, 11, 43]), and we emphasize that the validity of such a property is necessary for the formulation of the main conjecture of Iwasawa theory over a non-commutative p -adic Lie extension (see [5, 6, 8, 14, 25]). We should mention that at present, the only situation where the $\mathfrak{M}_H(G)$ property is known to hold is the “ $\mu = 0$ ” situation (for instance, see [8, Proposition 5.6], [11, Theorem 2.1] or [25, Lemma 2.9]), and the verification of the $\mathfrak{M}_H(G)$ -property in general seems out of reach at the moment (but see [9, Section 2], [11, Section 3] or [29, Section 3] for some related discussion in this direction). Granted this property and further suppose that H is pro- p without p -torsion, it then makes sense to speak of the $\mathcal{O}[[H]]$ -rank of the π -free quotient of the dual Selmer group, and this rank can be thought as a higher analog of the classical λ -invariant in the cyclotomic situation (for instance, see [22]).

We now present our key result. Let $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$ and $(B, \{B_v\}_{v|p}, \{B_v^+\}_{v|\mathbb{R}})$ be two data which satisfy the conditions (a)–(d) as in Section 3. Then one can attach dual Selmer groups to these data (see Section 3) which we denote by $X(A/F_\infty)$ and $X(B/F_\infty)$. We now introduce the following congruence condition on A and B which allows us to be able to compare the Selmer groups of A and B . (**Cong_n**) : There is an isomorphism $A[\pi^n] \cong B[\pi^n]$ of $\text{Gal}(\bar{F}/F)$ -modules which induces a $\text{Gal}(\bar{F}_v/F_v)$ -isomorphism $A_v[\pi^n] \cong B_v[\pi^n]$ for every $v|p$.

We define $e_G(A)$ to be

$$\min \left\{ r \mid \pi^r(X(A/F_\infty)(\pi)) = 0 \right\}.$$

Let S denote a finite set of primes of F which contains all the primes above p , the ramified primes of A and B , and the archimedean primes. The following is our main theorem (see Theorem 4.1.1 for a slightly refined version).

Theorem. *Let F_∞ be a strongly admissible pro- p p -adic Lie extension of F which is unramified outside S . Suppose that the following statements hold.*

- (1) (**Cong_{e_G(A)+1}**) holds.
- (2) $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property.
- (3) $X(B/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules.
- (4) For every $v \in S$, the decomposition group of G at v has dimension ≥ 2 .

Then $X(B/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property and we have

$$\text{rank}_{\mathcal{O}[[H]]}(X_f(A/F_\infty)) = \text{rank}_{\mathcal{O}[[H]]}(X_f(B/F_\infty)).$$

Statement (a) of the theorem can therefore be viewed as a generalization of the first assertion of [32, Theorem 4.2.1]. We mention that the equality in statement (b) of our main theorem has been established in [41, Theorem 8.8] for every specialization of a big Galois representation, but their proof relies on the much stronger assumption that the dual Selmer group of the big Galois representation satisfies the $\mathfrak{M}_H(G)$ -property (see Remark 4.3.3). We also note that our results apply to congruent Galois representations that need not be specialization of a big Galois representation, which their results do not apply.

We now say a little on the proof of the theorem, leaving the details to the rest of the paper. In the special case when the admissible p -extension is of dimension 2, statement (a) has been established by the author in [32, Proposition 5.1.3]. There we have to make use of a criterion of Coates and Sujatha (cf. [11, Corollary 3.2]; also see [32, Lemma 5.1.1]) which reduces the validity of $\mathfrak{M}_H(G)$ -property to certain relations on the μ -invariants. Statement (a) in this context then follows by combining this criterion of Coates-Sujatha with the author's comparison result (cf. [32, Theorem 4.2.1]) on the structure of the π -primary submodule of the dual Selmer groups of two congruent Galois representations over a general admissible p -adic Lie extension. However, the criterion of Coates and Sujatha is only stated for an admissible p -extension of dimension 2, and hence the above approach does not give a proof for the general situation. The main reason why we cannot extend the criterion of Coates and Sujatha to a general admissible p -adic Lie extension is that for a higher dimensional p -adic Lie extension, we have to account for the higher H -homology groups of the dual Selmer groups (for instance, see [29, Theorem 3.1]) which vanishes in the situation of dimension 2. At our present knowledge, it does not seem easy to study the structure of these homology groups (but see [29, Proposition 5.1] or [30, Proposition 4.3] for some discussion in this direction). Therefore, our proof of the main theorem *will* take a different route, and the proof is, perhaps surprisingly, not difficult. The approach of our proof is inspired by the proof in [1, Theorem 3.1]. The idea is to first relate an appropriate quotient of $X(A/F_\infty)$ with the mod π quotient of its π -free quotient (see Proposition 2.3.2). Under the congruence condition, we compare the former quotients of $X(A/F_\infty)$ and $X(B/F_\infty)$ up to finitely generated $k[[H]]$ -modules (here k is the residue field of \mathcal{O}). Then combining these with a Nakayama lemma argument, this in turn allows us to deduce the validity of the $\mathfrak{M}_H(G)$ -property of one from the other. The equality of the $\mathcal{O}[[H]]$ -ranks of the π -free quotient of $X(A/F_\infty)$ and $X(B/F_\infty)$ follows essentially from this argument with a finer analysis.

After proving our main theorem, we then apply it to study and compare the characteristic elements of π -free quotient of the dual Selmer groups (see Theorem 4.2.4). This latter result can be thought as a refinement of a previous result of the author in [30, Theorem 6.3]. We also apply our theorem to compare the Selmer groups of the specializations of a big Galois representation. Namely, we prove that for specializations in the big Galois representation which satisfy appropriate congruence condition, the dual Selmer group of one satisfies the $\mathfrak{M}_H(G)$ -property, then so will the other, and we have an equality of the ranks of the π -free quotients of the dual Selmer groups as predicted by Shekhar and Sujatha (see Theorem 4.3.2).

In short, the results in this paper are concerned with comparing the π -free quotient of the dual Selmer

groups of congruent Galois representations, and they complement the results proved by the author in [32] which is concerned with the comparison of the π -primary submodules of the dual Selmer groups. The combined results therefore give a rather satisfactory answer on comparing the dual Selmer groups of two congruent Galois representations when the congruence is a high power enough. At this point, it remains an open problem whether one can do any meaningful comparison of the dual Selmer groups when the Galois representations are congruent to each other by a power lower than the exponent of the π -primary submodules of the dual Selmer groups of the said Galois representations. To the best of the author knowledge, this issue does not seem to have been considered in literature, and unfortunately, the author also does not have a mean to do this at this point of writing. Another interesting problem is concerned with the situation of a big Galois representation. Despite being able to show the preservation of the $\mathfrak{M}_H(G)$ -property for appropriate specializations of the big Galois representation, we are not able to say anything on whether the dual Selmer group of the big Galois representation satisfies the $\mathfrak{M}_H(G)$ -property (in the sense of [11, Section 5]). In view of the noncommutative main conjecture for big Galois representations in the sense of [5], we strongly believe that these two problems are important questions of study and that the examination of these two problems will give insights towards understanding the noncommutative main conjecture for big Galois representations.

We now give a brief description of the layout of the paper. In Section 2, we recall certain algebraic notion which will be used subsequently in the paper. It is here where we develop a method to compare certain subquotients of two $\mathcal{O}[[G]]$ -modules which are annihilated by π^{n+1} from some n (see Proposition 2.2.3). We also identify certain subquotient of a $\mathcal{O}[[G]]$ -module with a quotient of its π -free quotient module (see Proposition 2.3.2), and this result paves a way for us to apply a Nakayama lemma argument. In Section 3, we introduce the Selmer groups which are the main object of study in this paper. Actually, to be precise, the Selmer group that we consider is called the strict Selmer group in Greenberg's terminology [16]. We will also introduce another variant of the Selmer group (called the Greenberg Selmer group) and an appropriate Selmer complex which is closely related to the strict Selmer group. In Section 4, we will present and prove all our main results. Finally, Appendix A contains some discussion on the non-existence of pseudo-null submodules of the dual (strict) Selmer group.

Acknowledgments. The author is supported by the National Natural Science Foundation of China under The Research Fund for International Young Scientists (Grant No: 11550110172).

2 Algebraic Preliminaries

In this section, we establish some algebraic preliminaries and notation which are necessary for us in order to prepare for the discussion and the proofs of our results.

2.1 Compact p -adic Lie group

Fix a prime p . In this subsection, we recall some facts about compact p -adic Lie groups. The standard references for the material presented here are [12, 28].

For a finitely generated pro- p group G , we write $G^{p^i} = \langle g^{p^i} \mid g \in G \rangle$, that is, the group generated by the p^i th-powers of elements in G . The pro- p group G is said to be *powerful* if $G/\overline{G^p}$ is abelian for odd p , or if $G/\overline{G^4}$ is abelian for $p = 2$. If a powerful pro- p group G is torsionfree, we say that G is *uniform* (cf. [12, Definition 4.1, Theorem 4.5]).

We now recall the following characterization of compact p -adic Lie groups due to Lazard [28] (see also [12, Corollary 8.34]): a topological group G is a compact p -adic Lie group if and only if G contains a open normal uniform pro- p subgroup. Furthermore, if G is a compact p -adic Lie group without p -torsion, it follows from [39, Corollaire 1] (see also [28, Chap. V Sect. 2.2]) that G has finite p -cohomological dimension.

2.2 Torsion modules and pseudo-null modules

As before, p will denote a fixed prime. Let \mathcal{O} be the ring of integers of a fixed finite extension of \mathbb{Q}_p . For a compact p -adic Lie group G , the completed group algebra of G over \mathcal{O} is given by

$$\mathcal{O}[[G]] = \varprojlim_U \mathcal{O}[G/U],$$

where U runs over the open normal subgroups of G and the inverse limit is taken with respect to the canonical projection maps.

When G is pro- p and has no p -torsion, it is well known that $\mathcal{O}[[G]]$ is an Auslander regular ring (cf. [44, Theorem 3.26] or [31, Theorem A.1]), and has no zero divisors (cf. [34]). Therefore, $\mathcal{O}[[G]]$ admits a skew field $K(G)$ which is flat over $\mathcal{O}[[G]]$ (see [15, Chapters 6 and 10] or [27, Chapter 4, §9 and §10]). If M is a finitely generated $\mathcal{O}[[G]]$ -module, we define the $\mathcal{O}[[G]]$ -rank of M to be

$$\text{rank}_{\mathcal{O}[[G]]}(M) = \dim_{K(G)} (K(G) \otimes_{\mathcal{O}[[G]]} M).$$

The $\mathcal{O}[[G]]$ -module M is then said to be *torsion* if $\text{rank}_{\mathcal{O}[[G]]} M = 0$. We will also make use of a well-known equivalent definition for M to be a torsion $\mathcal{O}[[G]]$ -module, namely: $\text{Hom}_{\mathcal{O}[[G]]}(M, \mathcal{O}[[G]]) = 0$ (for instance, see [31, Lemma 4.2] or [32, Lemma 2.2.1]). A finitely generated torsion $\mathcal{O}[[G]]$ -module M is said to be *pseudo-null* if $\text{Ext}_{\mathcal{O}[[G]]}^1(M, \mathcal{O}[[G]]) = 0$. For an equivalent definition, we refer readers to [44, Definitions 3.1 and 3.3; Proposition 3.5(ii)]. For the purpose of this article, the definition we adopt will suffice. Finally, we mention that every subquotient of a torsion $\mathcal{O}[[G]]$ -module (resp., pseudo-null $\mathcal{O}[[G]]$ -module) is also torsion (resp. pseudo-null).

Now, fix a local parameter π for \mathcal{O} and denote the residue field of \mathcal{O} by k . The completed group algebra of G over k is given by

$$k[[G]] = \varprojlim_U k[G/U],$$

where U runs over the open normal subgroups of G and the inverse limit is taken with respect to the canonical projection maps. For a compact p -adic Lie group G without p -torsion, it follows from [44, Theorem 3.30(ii)] (or [31, Theorem A.1]) that $k[[G]]$ is an Auslander regular ring. Furthermore, if G is pro- p , then the ring $k[[G]]$ has no zero divisors (cf. [2, Theorem C]). Therefore, one can define the notion

of $k[[G]]$ -rank as above when G is pro- p without p -torsion. Similarly, we will say that the module N is a *torsion* $k[[G]]$ -module if $\text{rank}_{k[[G]]} N = 0$.

We end the subsection with some algebraic results which will be used in the proof of our main result. As a start, we have the following simple observation.

Lemma 2.2.1. *Let H be a compact p -adic Lie group and M a compact $\mathcal{O}[[H]]$ -module. Suppose that M is annihilated by π^{n+1} . Then $M/M[\pi^n]$ and M/π^n are $k[[H]]$ -modules.*

Furthermore, if M is finitely generated over $\mathcal{O}[[H]]$, then $M/M[\pi^n]$ and M/π^n are finitely generated over $k[[H]]$.

Proof. It suffices to show that $M/M[\pi^n]$ and M/π^n are annihilated by π . Since $\pi^{n+1}M = 0$, we have $\pi m \in M[\pi^n]$ for all $m \in M$. This shows that $M/M[\pi^n]$ is annihilated by π .

By [38, Lemma 5.2.5(b)] and [47, Proposition 7.4.1], we have a surjection

$$\prod_I \mathcal{O}[[H]] \twoheadrightarrow M$$

for some index set I . Since M is annihilated by π^{n+1} , the surjection factors through a surjection

$$\prod_I \mathcal{O}[[H]]/\pi^{n+1} \twoheadrightarrow M.$$

It then follows from the following commutative diagram

$$\begin{array}{ccccc} \prod_I \mathcal{O}[[H]]/\pi^{n+1} & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow \pi^n & & \downarrow \pi^n & & \\ \prod_I \mathcal{O}[[H]]/\pi^{n+1} & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

that there is a surjection

$$\prod_I \mathcal{O}[[H]]/\pi \twoheadrightarrow M/\pi^n$$

which in turn implies that M/π^n is annihilated by π .

Finally, if M is finitely generated over $\mathcal{O}[[H]]$, so are $M/M[\pi^n]$ and M/π^n . But we have shown above that these two modules are annihilated by π , and hence they are finitely generated over $k[[H]]$. \square

For a closed subgroup U of a compact p -adic Lie group H and a compact $\mathcal{O}[[U]]$ -module M , we denote by $\text{Ind}_H^U(M) := M \hat{\otimes}_{\mathcal{O}[[U]]} \mathcal{O}[[H]]$ the compact induction of M from U to H . If M is a compact $k[[U]]$ -module, we can also view it as a compact $\mathcal{O}[[U]]$ -module and we have the identification $\text{Ind}_H^U(M) = M \hat{\otimes}_{k[[U]]} k[[H]]$.

Lemma 2.2.2. *Let H be a compact p -adic Lie group without p -torsion, U a closed subgroup of H and M a finite $\mathcal{O}[[U]]$ -module which is annihilated by π^{n+1} . Then $\text{Ind}_H^U(M)/\text{Ind}_H^U(M)[\pi^n]$ and $\text{Ind}_H^U(M)/\pi^n$ are finitely generated over $k[[H]]$.*

Furthermore, if U has dimension at least 1, then $\text{Ind}_H^U(M)/(\text{Ind}_H^U(M)[\pi^n])$ and $\text{Ind}_H^U(M)/\pi^n$ are finitely generated torsion $k[[H]]$ -modules.

Proof. Clearly, $\text{Ind}_H^U(M)$ is finitely generated over $\mathcal{O}[[H]]$ and is annihilated by π^{n+1} . Therefore, the first assertion follows from Lemma 2.2.1. Now consider the following exact sequence

$$0 \longrightarrow M[\pi^n] \longrightarrow M \xrightarrow{\pi^n} M \longrightarrow M/\pi^n \longrightarrow 0.$$

Since $\text{Ind}_H^U(-)$ is an exact functor (cf. [38, Lemma 6.10.8]), we have an exact sequence

$$0 \longrightarrow \text{Ind}_H^U(M)[\pi^n] \longrightarrow \text{Ind}_H^U(M) \xrightarrow{\pi^n} \text{Ind}_H^U(M) \longrightarrow \text{Ind}_H^U(M)/\pi^n \longrightarrow 0.$$

It now follows easily from this exact sequence that

$$\text{Ind}_H^U(M)/(\text{Ind}_H^U(M)[\pi^n]) \cong \text{Ind}_H^U(M/M[\pi^n])$$

and

$$\text{Ind}_H^U(M)/\pi^n \cong \text{Ind}_H^U(M/\pi^n).$$

Since M is finite, so are $M/M[\pi^n]$ and M/π^n . By Lemma 2.2.1, they are finite $k[[U]]$ -modules. Now if U has dimension at least 1, then $M/M[\pi^n]$ and M/π^n are torsion $k[[U]]$ -modules. The second assertion then follows from an application of an k -analog of [35, Lemma 5.5]. \square

The next proposition will be a key ingredient in our main theorem.

Proposition 2.2.3. *Let H be a compact p -adic Lie group which has no p -torsion and has dimension at least 1. Suppose that we are given an exact sequence*

$$0 \longrightarrow C \longrightarrow M \longrightarrow N \longrightarrow D \longrightarrow 0$$

of $k[[H]]$ -modules which are annihilated by π^{n+1} , where C is finitely generated over $\mathcal{O}[[H]]$ and D is finite. Then $M/M[\pi^n]$ is finitely generated over $k[[H]]$ if and only if $N/N[\pi^n]$ is finitely generated over $k[[H]]$.

Moreover, if $C/C[\pi^n]$ and C/π^n are finitely generated torsion $k[[H]]$ -modules, then we have

$$\text{rank}_{k[[H]]} M/M[\pi^n] = \text{rank}_{k[[H]]} N/N[\pi^n].$$

Proof. Write $P = \text{im}(M \longrightarrow N)$. We then have an exact sequence

$$0 \longrightarrow P[\pi^n] \longrightarrow N[\pi^n] \longrightarrow D[\pi^n] \longrightarrow P/\pi^n.$$

Denoting $U = \text{im}(N[\pi^n] \longrightarrow D[\pi^n])$, we then have the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & P[\pi^n] & \longrightarrow & N[\pi^n] & \longrightarrow & U \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & P & \longrightarrow & N & \longrightarrow & D \longrightarrow 0 \end{array}$$

with exact rows and the vertical maps are the inclusion maps. This in turn gives rise to the following short exact sequence

$$0 \longrightarrow P/P[\pi^n] \longrightarrow N/N[\pi^n] \longrightarrow D/U \longrightarrow 0.$$

By Lemma 2.2.1, this is an exact sequence of $k[[H]]$ -modules. Since D is finite, so is D/U . As H has dimension ≥ 1 , it follows that D/U is a finitely generated torsion $k[[H]]$ -module. Therefore, we have that $P/P[\pi^n]$ is finitely generated over $k[[H]]$ if and only if $N/N[\pi^n]$ is finitely generated over $k[[H]]$. Furthermore, in the event that these modules are finitely generated over $k[[H]]$, we have

$$\text{rank}_{k[[H]]} P/P[\pi^n] = \text{rank}_{k[[H]]} N/N[\pi^n].$$

Now consider the exact sequence

$$0 \longrightarrow C[\pi^n] \longrightarrow M[\pi^n] \longrightarrow P[\pi^n] \longrightarrow C/\pi^n.$$

Denote $V = \text{im}(M[\pi^n] \longrightarrow P[\pi^n])$ and $W = \text{im}(P[\pi^n] \longrightarrow C/\pi^n)$. We then have two commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C[\pi^n] & \longrightarrow & M[\pi^n] & \longrightarrow & V & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C & \longrightarrow & M & \longrightarrow & P & \longrightarrow & 0 \\ & & & & & & & & \\ 0 & \longrightarrow & V[\pi^n] & \longrightarrow & P[\pi^n] & \longrightarrow & W & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & & & \\ & & P & \xlongequal{\quad} & P & & & & \end{array}$$

with exact rows, where the vertical maps are the inclusion maps. From these two diagrams, we obtain two exact sequences

$$\begin{aligned} 0 \longrightarrow C/C[\pi^n] &\longrightarrow M/M[\pi^n] \longrightarrow P/V \longrightarrow 0 \\ 0 \longrightarrow W &\longrightarrow P/V \longrightarrow P/P[\pi^n] \longrightarrow 0. \end{aligned}$$

Since $W \subseteq C/\pi^n$, it follows from the assumption that C is finitely generated over $\mathcal{O}[[H]]$ and Lemma 2.2.1 that W and $C/C[\pi^n]$ are finitely generated over $k[[H]]$. Hence it follows from the two exact sequences that $M/M[\pi^n]$ is finitely generated over $k[[H]]$ if and only if $P/P[\pi^n]$ is finitely generated over $k[[H]]$. Combining this observation with that in the previous paragraph, we have that $M/M[\pi^n]$ is finitely generated over $k[[H]]$ if and only if $N/N[\pi^n]$ is finitely generated over $k[[H]]$.

Now if we assume further that $C/C[\pi^n]$ and C/π^n are finitely generated torsion $k[[H]]$ -modules, it then follows that W is also a finitely generated torsion $k[[H]]$ -module. By analysing the above two exact sequences again, we have

$$\text{rank}_{k[[H]]} M/M[\pi^n] = \text{rank}_{k[[H]]} P/P[\pi^n].$$

Combining this with the equality obtained at the end of the first paragraph of the proof, we obtained the desired equality. \square

We record another useful lemma.

Lemma 2.2.4. *Let H be a compact p -adic Lie group which has no p -torsion and has dimension at least 1. Let M be a finitely generated $\mathcal{O}[[H]]$ -module which is annihilated by π^{n+1} . Then we have the*

following statements. Suppose that $M/M[\pi^n]$ and M/π^n are torsion $k[[H]]$ -modules. Then for every $\mathcal{O}[[H]]$ -subquotient N of M , $N/N[\pi^n]$ and N/π^n are torsion $k[[H]]$ -modules.

Proof. It suffices to prove the assertion for the cases when N is submodule of M and when N is a quotient of M . Now suppose that $M \twoheadrightarrow N$. It is straightforward to verify that this surjection induces surjections $M/M[\pi^n] \twoheadrightarrow N/N[\pi^n]$ and $M/\pi^n \twoheadrightarrow N/\pi^n$. Hence $N/N[\pi^n]$ and N/π^n are torsion $k[[H]]$ -modules.

Now suppose that $N \subseteq M$. Then one can check easily that $N/N[\pi^n] \subseteq M/M[\pi^n]$, and so $N/N[\pi^n]$ is a torsion $k[[H]]$ -module. It therefore remains to show that N/π^n is a torsion $k[[H]]$ -module. Consider the following exact sequence

$$0 \longrightarrow N[\pi^n] \longrightarrow M[\pi^n] \longrightarrow P[\pi^n] \longrightarrow N/\pi^n \longrightarrow M/\pi^n \longrightarrow P/\pi^n \longrightarrow 0.$$

Denote $V = \text{im}(M[\pi^n] \longrightarrow P[\pi^n])$ and $W = \text{im}(P[\pi^n] \longrightarrow N/\pi^n)$. By a similar argument to that in Proposition 2.2.3, we obtain three exact sequences

$$\begin{aligned} 0 \longrightarrow N/N[\pi^n] \longrightarrow M/M[\pi^n] \longrightarrow P/V \longrightarrow 0, \\ 0 \longrightarrow W \longrightarrow P/V \longrightarrow P/P[\pi^n] \longrightarrow 0, \\ 0 \longrightarrow W \longrightarrow N/\pi^n \longrightarrow M/\pi^n \longrightarrow P/\pi^n \longrightarrow 0 \end{aligned}$$

of $k[[H]]$ -modules. (Note that by Lemma 2.2.1, $M/M[\pi^n]$ is a $k[[H]]$ -module, and hence, so are P/V and W .) Since $M/M[\pi^n]$ is a torsion $k[[H]]$ -module, it follows from the first two exact sequences that W is a torsion $k[[H]]$ -module. Combining this with the hypothesis that M/π^n is a torsion $k[[H]]$ -module, it follows from the third exact sequence that N/π^n is a torsion $k[[H]]$ -module. \square

2.3 μ -invariant and π -primary modules

For a given finitely generated $\mathcal{O}[[G]]$ -module M , we denote $M(\pi)$ to be the $\mathcal{O}[[G]]$ -submodule of M which consists of elements of M that are annihilated by some power of π . Since the ring $\mathcal{O}[[G]]$ is Noetherian, the module $M(\pi)$ is certainly finitely generated over $\mathcal{O}[[G]]$. Hence one can find an integer $r \geq 0$ such that π^r annihilates $M(\pi)$. The π -exponent of M is then defined to be

$$e_{\mathcal{O}[[G]]}(M) = \min\{r \mid \pi^r M(\pi) = 0\}.$$

Now suppose that G is pro- p without p -torsion. Following [22, Formula (33)], we define the μ -invariant

$$\mu_{\mathcal{O}[[G]]}(M) = \sum_{i \geq 0} \text{rank}_{k[[G]]}(\pi^i M(\pi)/\pi^{i+1}).$$

(For another alternative, but equivalent, definition, see [44, Definition 3.32].) By the above discussion and our definition of $k[[G]]$ -rank, the sum on the right is a finite one. It is clear from the definition that $\mu_{\mathcal{O}[[G]]}(M) = \mu_{\mathcal{O}[[G]]}(M(\pi))$. Also, it is not difficult to see that this definition coincides with the classical notion of the μ -invariant for Γ -modules when $G = \Gamma \cong \mathbb{Z}_p$.

Continue supposing that G is pro- p without p -torsion. Then both $\mathcal{O}[[G]]$ and $k[[G]]$ are Auslander regular rings with no zero divisors. For a finitely generated $\mathcal{O}[[G]]$ -module M , it then follows from [23, Proposition 1.11] (see also [44, Theorem 3.40]) that there is a $\mathcal{O}[[G]]$ -homomorphism

$$\varphi : M(\pi) \longrightarrow \bigoplus_{i=1}^s \mathcal{O}[[G]]/\pi^{\alpha_i},$$

whose kernel and cokernel are pseudo-null $\mathcal{O}[[G]]$ -modules, and where the integers s and α_i are uniquely determined. We will call $\bigoplus_{i=1}^s \mathcal{O}[[G]]/\pi^{\alpha_i}$ the *elementary representation* of $M(\pi)$. In fact, in the process of establishing the above, one also has the equality $\mu_{\mathcal{O}[[G]]}(M) = \sum_{i=1}^s \alpha_i$ (see loc. cit.). We will set

$$\theta_{\mathcal{O}[[G]]}(M) := \max_{1 \leq i \leq s} \{\alpha_i\}.$$

It is not difficult to see that $e_{\mathcal{O}[[G]]}(M) \geq \theta_{\mathcal{O}[[G]]}(M)$. The following lemma gives a sufficient criterion for equality to hold.

Lemma 2.3.1. *Let G be a compact p -adic Lie group which is pro- p and has no p -torsion. Suppose that M is a finitely generated $\mathcal{O}[[G]]$ -module which has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules. Then*

$$e_{\mathcal{O}[[G]]}(M) = \theta_{\mathcal{O}[[G]]}(M).$$

Proof. Let

$$\varphi : M(\pi) \longrightarrow \bigoplus_{i=1}^s \mathcal{O}[[G]]/\pi^{\alpha_i}$$

be an $\mathcal{O}[[G]]$ -homomorphism, whose kernel and cokernel are pseudo-null $\mathcal{O}[[G]]$ -modules. Since M has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules, it follows that φ is injective, and hence $\pi^{\theta_{\mathcal{O}[[G]]}(M)}$ annihilates $M(\pi)$. This in turn yields the required equality. \square

Finally, we introduce the notion of the $\mathfrak{M}_H(G)$ -property. Let G be a compact p -adic Lie group with a closed subgroup H such that $G/H \cong \mathbb{Z}_p$. We then say that a finitely generated $\mathcal{O}[[G]]$ -module M *satisfies the $\mathfrak{M}_H(G)$ -property* if its π -free quotient $M_f := M/M(\pi)$ is finitely generated over $\mathcal{O}[[H]]$. As noted in the introductory section, it has been conjectured for certain Galois representations coming from abelian varieties with good ordinary reduction at p or cuspidal eigenforms with good ordinary reduction at p , the dual Selmer group associated to such a Galois representation satisfies the $\mathfrak{M}_H(G)$ -property (see [8, 11, 14, 43]).

We end with another important proposition which will play a part in the proof of our main theorem. As mentioned in the introduction, the proposition and its proof are inspired by the proof of [1, Theorem 3.1]. The point of the proposition is to relate an appropriate quotient of M to the mod- π quotient of its π -free quotient.

Proposition 2.3.2. *Let G be a compact p -adic Lie group and H a closed subgroup of G such that $G/H \cong \mathbb{Z}_p$. Let M be a finitely generated torsion $\mathcal{O}[[G]]$ -module. Then for every $n \geq 1$, we have a short exact sequence*

$$0 \longrightarrow \frac{M(\pi)/\pi^{n+1}}{(M(\pi)/\pi^{n+1})[\pi^n]} \longrightarrow \frac{M/\pi^{n+1}}{(M/\pi^{n+1})[\pi^n]} \longrightarrow M_f/\pi \longrightarrow 0$$

of finitely generated $k[[G]]$ -modules (and hence compact $k[[H]]$ -modules). In particular, when $n \geq e_{\mathcal{O}[[G]]}(M)$, we have an isomorphism

$$\frac{M/\pi^{n+1}}{(M/\pi^{n+1})[\pi^n]} \cong M_f/\pi$$

of finitely generated $k[[G]]$ -modules (and hence compact $k[[H]]$ -modules).

Proof. Consider the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M(\pi) & \longrightarrow & M & \longrightarrow & M_f & \longrightarrow & 0 \\ & & \downarrow \pi^n & & \downarrow \pi^n & & \downarrow \pi^n & & \\ 0 & \longrightarrow & M(\pi) & \longrightarrow & M & \longrightarrow & M_f & \longrightarrow & 0 \end{array}$$

with exact rows, where the vertical maps are given by multiplication by π^n . Since M_f has no π -torsion, the rightmost vertical map is injective. Therefore, it follows that there is a short exact sequence

$$0 \longrightarrow M(\pi)/\pi^n \longrightarrow M/\pi^n \longrightarrow M_f/\pi^n \longrightarrow 0$$

of $\mathcal{O}[[G]]$ -modules. We also have a similar short exact sequence replacing n by $n+1$. This latter short exact sequence gives rise to a long exact sequence

$$0 \longrightarrow (M(\pi)/\pi^{n+1})[\pi^n] \longrightarrow (M/\pi^{n+1})[\pi^n] \longrightarrow (M_f/\pi^{n+1})[\pi^n] \longrightarrow M(\pi)/\pi^n \longrightarrow M/\pi^n \longrightarrow M_f/\pi^n \longrightarrow 0.$$

Since the three terms on the right is part of the former short exact sequence, we deduce that the first three terms of the long exact sequence actually form a short exact sequence

$$0 \longrightarrow (M(\pi)/\pi^{n+1})[\pi^n] \longrightarrow (M/\pi^{n+1})[\pi^n] \longrightarrow (M_f/\pi^{n+1})[\pi^n] \longrightarrow 0.$$

It then follow from this that we have a short exact sequence

$$0 \longrightarrow \frac{M(\pi)/\pi^{n+1}}{(M(\pi)/\pi^{n+1})[\pi^n]} \longrightarrow \frac{M/\pi^{n+1}}{(M/\pi^{n+1})[\pi^n]} \longrightarrow \frac{M_f/\pi^{n+1}}{(M_f/\pi^{n+1})[\pi^n]} \longrightarrow 0$$

of $k[[G]]$ -modules (noting Lemma 2.2.1). It remains to show that

$$\frac{M_f/\pi^{n+1}}{(M_f/\pi^{n+1})[\pi^n]} \cong M_f/\pi.$$

But this is not difficult to show. In fact, as M_f has no π -torsion, one can easily check that

$$(M_f/\pi^{n+1})[\pi^n] = \pi M_f/\pi^{n+1},$$

and the required isomorphism is immediate from this.

Finally, if $n \geq e_{\mathcal{O}[[G]]}(M)$, then

$$\frac{M(\pi)/\pi^{n+1}}{(M(\pi)/\pi^{n+1})[\pi^n]} = \frac{M(\pi)}{M(\pi)} = 0.$$

The proof of the proposition is now completed. \square

We record one more result which gives an upper bound of the π -exponent..

Proposition 2.3.3. *Let G be a compact p -adic Lie group and H a closed subgroup of G such that $G/H \cong \mathbb{Z}_p$. Let M be a finitely generated torsion $\mathcal{O}[[G]]$ -module which has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules. Suppose that $\frac{M/\pi^{n+1}}{(M/\pi^{n+1})[\pi^n]}$ is finitely generated over $k[[H]]$ for some n . Then we have $\theta_{\mathcal{O}[[G]]}(M) = e_{\mathcal{O}[[G]]}(M) \leq n$. In particular, we have an isomorphism*

$$\frac{M/\pi^{n+1}}{(M/\pi^{n+1})[\pi^n]} \cong M_f/\pi$$

of finitely generated $k[[G]]$ -modules (and hence compact $k[[H]]$ -modules).

Proof. The first equality is a consequence of Lemma 2.3.1. We now proceed with proving $\theta_{\mathcal{O}[[G]]}(M) \leq n$. By Proposition 2.3.2, $\frac{M(\pi)/\pi^{n+1}}{(M(\pi)/\pi^{n+1})[\pi^n]}$ is finitely generated over $k[[H]]$, and hence over $\mathcal{O}[[H]]$. Thus, this module has trivial $\mu_{\mathcal{O}[[G]]}$ -invariant (cf. [22, Lemma 2.7]). This in turn implies that

$$\mu_{\mathcal{O}[[G]]}\left(M(\pi)/\pi^{n+1}\right) = \mu_{\mathcal{O}[[G]]}\left((M(\pi)/\pi^{n+1})[\pi^n]\right).$$

Consider an $\mathcal{O}[[G]]$ -homomorphism

$$\varphi : M(\pi) \longrightarrow \bigoplus_{i=1}^s \mathcal{O}[[G]]/\pi^{\alpha_i},$$

whose kernel and cokernel are pseudo-null $\mathcal{O}[[G]]$ -modules. Then it is straightforward to verify that φ induces two $\mathcal{O}[[G]]$ -homomorphisms

$$M(\pi)/\pi^{n+1} \longrightarrow \bigoplus_{i=1}^s \mathcal{O}[[G]]/\pi^{\min\{n+1, \alpha_i\}}$$

and

$$(M(\pi)/\pi^{n+1})[\pi^n] \longrightarrow \bigoplus_{i=1}^s \mathcal{O}[[G]]/\pi^{\min\{n, \alpha_i\}},$$

whose kernels and cokernels are pseudo-null $\mathcal{O}[[G]]$ -modules. Since the two modules in question have the same $\mu_{\mathcal{O}[[G]]}$ -invariants by the above discussion, we have an equality

$$\sum_{i=1}^s \min\{n, \alpha_i\} = \sum_{i=1}^s \min\{n+1, \alpha_i\}$$

which in turn implies that $\alpha_i \leq n$ for all i . Hence $e_{\mathcal{O}[[G]]}(M) = \theta_{\mathcal{O}[[G]]}(M) \leq n$. This proves the first assertion of the proposition. The second assertion of the proposition is then immediate from this and Proposition 2.3.2. \square

3 Arithmetic Preliminaries

In this section, we introduce the Selmer groups and Selmer complexes. At the same time, we fix the notation that we shall use throughout the paper.

3.1 Arithmetic datum

To start, let p be a prime and F a number field. If $p = 2$, assume further that our number field F has no real primes. Denote by \mathcal{O} the ring of integers of some finite extension K of \mathbb{Q}_p . We then fix a local parameter π for \mathcal{O} . Suppose that we are given the following datum $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$ defined over F :

- (a) A is a cofree \mathcal{O} -module of \mathcal{O} -corank d with a continuous, \mathcal{O} -linear $\text{Gal}(\bar{F}/F)$ -action which is unramified outside a finite set of primes of F .
- (b) For each prime v of F above p , A_v is a $\text{Gal}(\bar{F}_v/F_v)$ -submodule of A which is cofree of \mathcal{O} -corank d_v .
- (c) For each real prime v of F , we write $A_v^+ = A^{\text{Gal}(\bar{F}_v/F_v)}$ which is assumed to be cofree of \mathcal{O} -corank d_v^+ .
- (d) The quantities d, d_v and d_v^+ satisfy the following identity

$$\sum_{v|p} (d - d_v)[F_v : \mathbb{Q}_p] = dr_2(F) + \sum_{v \text{ real}} (d - d_v^+), \quad (1)$$

where $r_2(F)$ is the number of complex primes of F .

We now consider the base change property of our datum. Let L be a finite extension of F . We can then obtain another datum $(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}})$ over L as follows: we consider A as a $\text{Gal}(\bar{F}/L)$ -module, and for each prime w of L above p , we set $A_w = A_v$, where v is a prime of F below w , and view it as a $\text{Gal}(\bar{F}_w/L_w)$ -module. Then $d_w = d_v$. For each real prime w of L , one sets $A^{\text{Gal}(\bar{L}_w/L_w)} = A^{\text{Gal}(\bar{F}_v/F_v)}$ and writes $d_w^+ = d_v^+$, where v is a real prime of F below w . In general, the d_w 's and d_w^+ 's need not satisfy equality (2). We now record the following lemma which gives some sufficient conditions for equality (2) to hold for the datum $(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}})$ over L .

Lemma 3.1.1. *Suppose that $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$ is a datum defined over F . Suppose further that at least one of the following statements holds.*

- (i) *All the archimedean primes of F are unramified in L .*
- (ii) *$[L : F]$ is odd*
- (iii) *F is totally imaginary.*

(iv) F is totally real, L is totally imaginary and

$$\sum_{v \text{ real}} d_v^+ = d[F : \mathbb{Q}]/2.$$

Then we have the equality

$$\sum_{w|p} (d - d_w)[L_w : \mathbb{Q}_p] = dr_2(L) + \sum_{w \text{ real}} (d - d_w^+).$$

Proof. Since the only ramified archimedean primes are real primes and real primes can only ramify in an extension of even degree, it follows that if either of the assertions in (ii) or (iii) holds, then the assertion in (i) holds. Therefore, to prove the lemma in these cases, it suffices to prove it under the assumption of (i). We first perform the following calculation

$$\begin{aligned} \sum_{w|p} (d - d_w)[L_w : \mathbb{Q}_p] &= \sum_{v|p} \sum_{w|v} (d - d_v)[L_w : F_v][F_v : \mathbb{Q}_p] \\ &= \sum_{v|p} (d - d_v)[F_v : \mathbb{Q}_p] \sum_{w|v} [L_w : F_v] \\ &= [L : F] \sum_{v|p} (d - d_v)[F_v : \mathbb{Q}_p] \\ &= [L : F] \left(dr_2(F) + \sum_{v \text{ real}} (d - d_v^+) \right) \\ &= d[L : F]r_2(F) + [L : F] \sum_{v \text{ real}} (d - d_v^+). \end{aligned}$$

Now if (i) holds, then every prime of L above a real prime (resp., complex prime) of F is a real prime (resp., complex prime). Therefore, one has $[L : F]r_2(F) = r_2(L)$ and

$$[L : F] \sum_{v \text{ real}} (d - d_v^+) = \sum_{w \text{ real}} (d - d_w^+).$$

The required conclusion then follows.

Now suppose that (iv) holds. Then $r_2(F) = 0$ and we have

$$\begin{aligned} \sum_{w|p} (d - d_w)[L_w : \mathbb{Q}_p] &= [L : F] \sum_{v \text{ real}} (d - d_v^+) = [L : F] \sum_{v \text{ real}} d - [L : F] \sum_{v \text{ real}} d_v^+ \\ &= [L : F][F : \mathbb{Q}]d - [L : F]d[F : \mathbb{Q}]/2 \\ &= d[L : \mathbb{Q}]/2 = dr_2(L). \end{aligned}$$

□

We now describe the arithmetic situation, where we can obtain the datum from. Let V be a d -dimensional K -vector space with a continuous $\text{Gal}(\bar{F}/F)$ -action which is unramified outside a finite set of primes. Suppose that for each prime v of F above p , there is a d_v -dimensional K -subspace V_v of V which is invariant under the action of $\text{Gal}(\bar{F}_v/F_v)$, and for each real prime v of F , $V^{\text{Gal}(\bar{F}_v/F_v)}$ has

dimension d_v^+ . Choose a $\text{Gal}(\bar{F}/F)$ -stable \mathcal{O} -lattice T of V (such a lattice exists by compactness). We can obtain a datum as above from V by setting $A = V/T$ and $A_v = V_v/T \cap V_v$. Note that both A and A_v depend on the choice of the lattice T . The basic examples of such Galois representations are (1) $V = V_p(E)$, where E is an elliptic curve with either good ordinary reduction or multiplicative reduction at each prime of F above p , (2) V is the Galois representation attached to a primitive Hecke eigenform which is ordinary at p . For more examples of how the above datum arises from Galois representations, we refer readers to [16, §9], [46, Section 1.2] and [32, Section 3].

3.2 Selmer groups

We now introduce two variants of Selmer groups due to Greenberg [16]. Let S be a finite set of primes of F which contains all the primes above p , the ramified primes of A and all the infinite primes of F . Denote by F_S the maximal algebraic extension of F unramified outside S and write $G_S(\mathcal{L}) = \text{Gal}(F_S/\mathcal{L})$ for every algebraic extension \mathcal{L} of F which is contained in F_S . Let L be a finite extension of F contained in F_S such that the datum $(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}})$ satisfies (2). For a prime w of L lying over S , set

$$H_{str}^1(L_w, A) = \begin{cases} \ker(H^1(L_w, A) \longrightarrow H^1(L_w, A/A_w)) & \text{if } w \text{ divides } p, \\ \ker(H^1(L_w, A) \longrightarrow H^1(L_w^{ur}, A)) & \text{if } w \text{ does not divide } p, \end{cases}$$

where L_w^{ur} is the maximal unramified extension of L_w . The (strict) Selmer group attached to the datum is then defined by

$$S(A/L) := \text{Sel}^{str}(A/L) := \ker\left(H^1(G_S(L), A) \longrightarrow \bigoplus_{w \in S_L} H_s^1(L_w, A)\right),$$

where we write $H_s^1(L_w, A) = H^1(L_w, A)/H_{str}^1(L_w, A)$ and S_L denotes the set of primes of L above S . We then write $X(A/L)$ for the Pontryagin dual of $S(A/L)$.

A Galois extension F_∞ of F is said to be an *S -admissible p -adic Lie extension* of F if (i) $\text{Gal}(F_\infty/F)$ is compact p -adic Lie group, (ii) F_∞ contains the cyclotomic \mathbb{Z}_p extension F_{cyc} of F and (iii) F_∞ is contained in F_S . Write $G = \text{Gal}(F_\infty/F)$, $H = \text{Gal}(F_\infty/F_{cyc})$ and $\Gamma = \text{Gal}(F_{cyc}/F)$. In the event that $\text{Gal}(F_\infty/F)$ is a compact p -adic Lie group without p -torsion, we say that F_∞ is a *strongly S -admissible p -adic Lie extension* of F .

We define $S(A/F_\infty) = \varinjlim_L S(A/L)$, where the limit runs over all finite extensions L of F contained in F_∞ . We shall write $X(A/F_\infty)$ for the Pontryagin dual of $S(A/F_\infty)$. By a similar argument to that in [11, Corollary 2.3], one can show that $X(A/F_\infty)$ is independent of the choice of S as long as S contains all the primes above p , the ramified primes of A , the primes that ramify in F_∞/F and all infinite primes.

We introduce another variant of the Selmer group which is usually called the Greenberg Selmer group. Set

$$H_{Gr}^1(F_v, A) = \begin{cases} \ker(H^1(F_v, A) \longrightarrow H^1(F_v^{ur}, A/A_v)) & \text{if } v|p, \\ \ker(H^1(F_v, A) \longrightarrow H^1(F_v^{ur}, A)) & \text{if } v \nmid p. \end{cases}$$

The Greenberg Selmer group attached to the datum $(A, \{A_w\}_{w|p}, \{A_w^+\}_{w|\mathbb{R}})$ is then defined by

$$\mathrm{Sel}^{Gr}(A/F) = \ker \left(H^1(G_S(F), A) \longrightarrow \bigoplus_{v \in S} H_g^1(F_v, A) \right),$$

where we write $H_g^1(F_v, A) = H^1(F_v, A)/H_{Gr}^1(F_v, A)$. For an S -admissible p -adic Lie extension F_∞ , we define $\mathrm{Sel}^{Gr}(A/F_\infty) = \varinjlim_L \mathrm{Sel}^{Gr}(A/L)$ and denote by $X^{Gr}(A/F_\infty)$ the Pontryagin dual of $\mathrm{Sel}^{Gr}(A/F_\infty)$.

We end the subsection by comparing the two Selmer groups of Greenberg which will take the form of two lemmas.

Lemma 3.2.1. *We have an exact sequence*

$$0 \longrightarrow N \longrightarrow X^{Gr}(A/F_\infty) \longrightarrow X(A/F_\infty) \longrightarrow 0,$$

where N is a finitely generated $\mathcal{O}[[H]]$ -module.

Suppose further that for each $v|p$, the decomposition group of $G = \mathrm{Gal}(F_\infty/F)$ at v has dimension ≥ 2 . Then N is a finitely generated torsion $\mathcal{O}[[H]]$ -module.

Proof. Consider the following commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & S(A/F_\infty) & \longrightarrow & H^1(G_S(F_\infty), A) & \longrightarrow & \bigoplus_{v \in S} J_v(A/F_\infty) \\ & & \downarrow & & \parallel & & \downarrow \alpha \\ 0 & \longrightarrow & \mathrm{Sel}^{Gr}(A/F_\infty) & \longrightarrow & H^1(G_S(F_\infty), A) & \longrightarrow & \bigoplus_{v \in S} J_v^{Gr}(A/F_\infty) \end{array}$$

with exact rows, where $J_v^{Gr}(A/F_\infty) = \varinjlim_L \bigoplus_{w|v} H_g^1(L_w, A)$. We first show that $\ker \alpha$ is cofinitely generated over $\mathcal{O}[[H]]$. Write $\alpha = \bigoplus_v \alpha_v$, where v runs over the set of primes of F above S . Clearly, $J_v(A/F_\infty) = J_v^{Gr}(A/F_\infty)$ for $v \nmid p$. Therefore, $\ker \alpha_v = 0$ for these v 's.

Now for each $v|p$, write $\alpha_v = \bigoplus_w \alpha_w$, where w runs over the set of primes of F^{cyc} above v . Fix a prime of F_∞ above v which we will also denote by w . Write $I_{\infty, w}$ for the inertia subgroup of $\mathrm{Gal}(\overline{F}_{\infty, w}/F_{\infty, w})$ and $U_w = \mathrm{Gal}(\overline{F}_{\infty, w}/F_{\infty, w})/I_{\infty, w}$. It then follows from the Hochschild-Serre spectral sequence that we have

$$0 \longrightarrow H^1(U_w, (A/A_v)^{I_{\infty, w}}) \longrightarrow H^1(F_{\infty, w}, A/A_v) \longrightarrow H^1(I_{\infty, w}, A/A_v)^{U_w}.$$

Since U_w is topologically cyclic, $H^1(U_w, (A/A_v)^{I_{\infty, w}}) \cong ((A/A_v)^{I_{\infty, w}})_{U_w}$ and so is cofinitely generated over \mathcal{O} . Let H_w denote the decomposition subgroup of H corresponding to w . Then $\ker \alpha_w = \mathrm{Coind}_H^{H_w}(H^1(U_w, (A/A_v)^{I_{\infty, w}}))$ is cofinitely generated over $\mathcal{O}[[H]]$. Since there is only finite number of primes of F^{cyc} above v , we have that $\ker \alpha_v$ is cofinitely generated over $\mathcal{O}[[H]]$.

Now suppose that for each $v|p$, the decomposition group of $G = \mathrm{Gal}(F_\infty/F)$ at v has dimension ≥ 2 . Then H_w has dimension ≥ 1 , and it follows from this that $H^1(U_w, (A/A_v)^{I_{\infty, w}})$ is a cofinitely generated torsion $\mathcal{O}[[H_w]]$ -module. By [35, Lemma 5.5], this in turn implies that $\ker \alpha_v$ is a cofinitely generated torsion $\mathcal{O}[[H]]$ -module. \square

In the next lemma, we will write $X_f(A/F_\infty)$ (resp., $X_f^{Gr}(A/F_\infty)$) for the π -free quotient of $X(A/F_\infty)$ (resp., the π -free quotient of $X^{Gr}(A/F_\infty)$).

Lemma 3.2.2. *$X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property if and only if $X^{Gr}(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property.*

Suppose further that $G = \text{Gal}(F_\infty/F)$ is pro- p without p -torsion and that for each $v|p$, the decomposition group of G at v has dimension ≥ 2 . Then if $X(A/F_\infty)$ (and hence $X^{Gr}(A/F_\infty)$) satisfies the $\mathfrak{M}_H(G)$ -property, we have

$$\text{rank}_{\mathcal{O}[[H]]}(X_f(A/F_\infty)) = \text{rank}_{\mathcal{O}[[H]]}(X_f^{Gr}(A/F_\infty)).$$

Proof. We first verify the first assertion of the lemma. By the first assertion of Lemma 3.2.1, we have an exact sequence

$$0 \longrightarrow N \longrightarrow X^{Gr}(A/F_\infty) \longrightarrow X(A/F_\infty) \longrightarrow 0,$$

where N is a finitely generated $\mathcal{O}[[H]]$ -module. For notational simplicity, we write $X = X(A/F_\infty)$ and $X^{Gr} = X^{Gr}(A/F_\infty)$. For a sufficiently large n , we have $Z(\pi) = Z[\pi^n]$ for $Z = N, X^{Gr}, X$. We then have an exact sequence

$$0 \longrightarrow N(\pi) \longrightarrow X^{Gr}(\pi) \longrightarrow X(\pi) \longrightarrow N/\pi^n.$$

Write $B = \text{im}(X^{Gr}(\pi) \longrightarrow X(\pi))$ and $C = \text{im}(X(\pi) \longrightarrow N/\pi^n)$. Consider the following two commutative diagrams

$$\begin{array}{ccccccc} 0 & \longrightarrow & N(\pi) & \longrightarrow & X^{Gr}(\pi) & \longrightarrow & B \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & N & \longrightarrow & X^{Gr} & \longrightarrow & X \longrightarrow 0 \\ & & & & & & \\ 0 & \longrightarrow & B & \longrightarrow & X(\pi) & \longrightarrow & C \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \\ & & X & \xlongequal{\quad} & X & & \end{array}$$

with exact rows, where the vertical maps are the inclusion maps. From these two diagrams, we obtain two exact sequences

$$\begin{aligned} 0 &\longrightarrow N_f \longrightarrow X_f^{Gr} \longrightarrow X/B \longrightarrow 0 \\ 0 &\longrightarrow C \longrightarrow X/B \longrightarrow X_f \longrightarrow 0. \end{aligned}$$

Since N is finitely generated over $\mathcal{O}[[H]]$, it follows that N_f and C are finitely generated over $\mathcal{O}[[H]]$. Hence it follows from the two exact sequences that X_f^{Gr} is finitely generated over $\mathcal{O}[[H]]$ if and only if X_f is finitely generated over $\mathcal{O}[[H]]$. This is precisely what we want to show.

Finally, we note that since N is torsion over $\mathcal{O}[[H]]$ by the second assertion of Lemma 3.2.1, so are N_f and C . The second assertion of the lemma is then immediate from analysing the two exact sequences in the previous paragraph. \square

3.3 Selmer complexes

The notion of a Selmer complex was first conceived and introduced in [33]. In our discussion, we consider a modified version of the Selmer complex as given in [14, 4.2.11] (also see [5, Section 3.1]). There are several advantages for using Selmer complexes in the formulation of the main conjecture rather than the Pontryagin dual of the Selmer group. We will just mention two of these as word of mouth (for more details, see [6, 14, 33]). Firstly, Selmer complexes have better functorial properties than Selmer groups, and secondly, Nekovář has shown that the Selmer complex is able to explain certain phenomena concerning about the trivial zeroes (see [33, 0.10]).

We now give the definition of the Selmer complex associated to the datum $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$. Write $T^* = \text{Hom}_{\text{cts}}(A, \mu_{p^\infty})$ and $T_v^* = \text{Hom}_{\text{cts}}(A/A_v, \mu_{p^\infty})$. For every finite extension L of F and w a prime of L above p , write $T_w^* = T_v^*$, where v is the prime of F below w . For any profinite group \mathcal{G} and a topological abelian group M with a continuous \mathcal{G} -action, we denote by $C(\mathcal{G}, M)$ the complex of continuous cochains of \mathcal{G} with coefficients in M . Let F_∞ be an S -admissible extension of F with Galois group G . We define a $(\mathcal{O}[[G]])[G_S(F)]$ -module $\mathcal{F}_G(T^*)$ as follows: as an \mathcal{O} -module, $\mathcal{F}_G(T^*) = \mathcal{O}[[G]] \otimes_{\mathcal{O}} T^*$, and the action of $G_S(F)$ is given by the formula $\sigma(x \otimes t) = x\bar{\sigma}^{-1} \otimes \sigma t$, where $\bar{\sigma}$ is the canonical image of σ in $G \subseteq \mathcal{O}[[G]]$. We define the $(\mathcal{O}[[G]])[\text{Gal}(\bar{F}_v/F_v)]$ -module $\mathcal{F}_G(T_v^*)$ in a similar fashion.

For every prime v of F , we write $C(F_v, \mathcal{F}_G(T^*)) = C(\text{Gal}(\bar{F}_v/F_v), \mathcal{F}_G(T^*))$. For each prime v not dividing p , denote $C_f(F_v, \mathcal{F}_G(T^*))$ to be the subcomplex of $C(F_v, \mathcal{F}_G(T^*))$, whose degree m -component is 0 unless $m \neq 0, 1$, whose degree 0-component is $C^0(F_v, \mathcal{F}_G(T^*))$, and whose degree 1-component is

$$\ker \left(C^1(F_v, \mathcal{F}_G(T^*))_{d=0} \longrightarrow H^1(F_v^{ur}, \mathcal{F}_G(T^*)) \right).$$

The Selmer complex $SC(T^*, T_v^*)$ is then defined to be

$$\text{Cone} \left(C(G_S(F), \mathcal{F}_G(T^*)) \longrightarrow \bigoplus_{v|p} C(F_v, \mathcal{F}_G(T^*)/\mathcal{F}_G(T_v^*)) \oplus \bigoplus_{v \nmid p} C(F_v, \mathcal{F}_G(T^*)) / C_f(F_v, \mathcal{F}_G(T^*)) \right) [-1].$$

Here $[-1]$ is the translation by -1 of the complex. We will write $H^i(SC(T^*, T_v^*))$ for the i th cohomology group of the Selmer complex $SC(T^*, T_v^*)$. We now state the following fundamental proposition which describes the relationship between the Selmer complex, or more precisely, its cohomology with the Selmer groups. For its proof, we refer readers to [14, Proposition 4.2.35].

Proposition 3.3.1. *Let \mathcal{G} be the kernel of $\text{Gal}(\bar{F}/F) \longrightarrow G$. For a place v of F , fixing an embedding $F \hookrightarrow F_v$, let $\mathcal{G}(v)$ be the kernel of $\text{Gal}(\bar{F}_v/F_v) \longrightarrow G$ and let $G_v \subseteq G$ be the image. Then the following statements hold.*

(a) $H^i(SC(T^*, T_v^*)) = 0$ for $i \neq 1, 2, 3$.

(b) We have an exact sequence

$$\begin{aligned} 0 \longrightarrow X(A/F_\infty) \longrightarrow H^2(SC(T^*, T_v^*)) &\longrightarrow \bigoplus_{v|p} \mathcal{O}[[G]] \otimes_{\mathcal{O}[[G_v]]} (T_v^*(-1))_{\mathcal{G}(v)} \\ &\longrightarrow (T^*(-1))_{\mathcal{G}} \longrightarrow H^3(SC(T^*, T_v^*)) \longrightarrow 0. \end{aligned}$$

In the next lemma, we write $H^2(SC(T^*, T_v^*))_f$ for the π -free quotient of $H^2(SC(T^*, T_v^*))$.

Lemma 3.3.2. *$X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property if and only if $H^2(SC(T^*, T_v^*))$ satisfies the $\mathfrak{M}_H(G)$ -property.*

Suppose further that $G = \text{Gal}(F_\infty/F)$ is pro- p without p -torsion and that for each $v|p$, the decomposition group of G at v has dimension ≥ 2 . Then if $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property, we have

$$\text{rank}_{\mathcal{O}[[H]]}(X_f(A/F_\infty)) = \text{rank}_{\mathcal{O}[[H]]}\left(H^2(SC(T^*, T_v^*))_f\right).$$

Proof. Since F_∞ contains F_{cyc} , it follows that for every prime $v|p$, the group G_v has dimension at least 1. Therefore, $\bigoplus_{v|p} \mathcal{O}[[G]] \otimes_{\mathcal{O}[[G_v]]} (T_v^*(-1))_{\mathcal{G}(v)}$ is finitely generated over $\mathcal{O}[[H]]$. Now if for each $v|p$, the decomposition group of G at v has dimension ≥ 2 , then this is in fact a finitely generated torsion $\mathcal{O}[[H]]$ -module. The conclusion of the lemma now follows from a similar argument to that in Lemma 3.2.2. \square

We end the section with the following remark.

Remark 3.3.3. Retain all the assumptions of Lemma 3.3.2. By the exact sequence in Proposition 3.3.1, we have that $H^3(SC(T^*, T_v^*))$ is finitely generated over \mathcal{O} . In particular, this implies that $H^3(SC(T^*, T_v^*))$ is finitely generated torsion over $\mathcal{O}[[H]]$. Now since $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property, it follows from an application of [14, Proposition 4.3.11] that $H^1(SC(T^*, T_v^*)) = 0$. Combining the above discussion with [32, Lemma 3.3.2], we see that $X(A/F_\infty)$ captures much of the essential Iwasawa invariants (namely, the structure of π -primary submodules, the $\mathfrak{M}_H(G)$ -property and the $\mathcal{O}[[H]]$ -rank of the π -free quotient) of the Selmer complex $SC(T^*, T_v^*)$ and vice versa.

4 Main results

In this section, we will prove the main theorem of the paper. We will then apply our theorem to study the specialization of a big Galois representation. For the remainder of the paper, we will work with $X(A/F_\infty)$. In view of Lemmas 3.2.2 and 3.3.2, there are also results for the Greenberg Selmer groups and the second cohomology of the Selmer complexes analogous to Theorems 4.1.1 and 4.3.2. We will only state formally the results for the Greenberg strict Selmer groups, leaving the cases of the Greenberg Selmer groups and Selmer complexes for the readers to fill in.

4.1 Congruent Galois representations

As before, let p be a prime. We let F be a number field. **If $p = 2$, we assume further that F has no real primes.** Let $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$ and $(B, \{B_v\}_{v|p}, \{B_v^+\}_{v|\mathbb{R}})$ be two data which satisfy the conditions (a)–(d) as in Section 3. From now on, S will always denote a finite set of primes of F which contains all the primes above p , the ramified primes of A and B , and the archimedean primes. As before, for a given S -admissible p -adic Lie-extension F_∞ of F , we write $G = \text{Gal}(F_\infty/F)$ and $H = \text{Gal}(F_\infty/F^{\text{cyc}})$.

We will also assume that the data obtained by base change over every finite extension of L of F in F_∞ also satisfy the conditions (a)–(d). Note that this assumption is automatically satisfied when F_∞ is a pro- p extension of F by Lemma 3.1.1 (and noting our standing assumption that if $p = 2$, then F has no real primes).

We now introduce the following important congruence condition on A and B which allows us to be able to compare the Selmer groups of A and B .

(Cong_n) : There is an isomorphism $A[\pi^n] \cong B[\pi^n]$ of $G_S(F)$ -modules which induces a $\text{Gal}(\bar{F}_v/F_v)$ -isomorphism $A_v[\pi^n] \cong B_v[\pi^n]$ for every $v|p$.

To simplify notation, we will write $e_G(A) = e_{\mathcal{O}[[G]]}(X(A/F_\infty))$. The following is the first main theorem of the paper.

Theorem 4.1.1. *Let F_∞ be an S -admissible p -adic Lie extension of F . Suppose that the following statements hold.*

- (1) **(Cong_{e_G(A)+1})** holds.
- (2) $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property.
- (3) $X(B/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules.

Then we have the following statements.

- (a) $X(B/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property.
- (b) Suppose further that the following statements hold.
 - (i) F_∞ is a strongly S -admissible pro- p p -adic Lie extension of F .
 - (ii) For every $v \in S$, the decomposition group of G at v has dimension ≥ 2 .

Then we have

$$\text{rank}_{\mathcal{O}[[H]]}(X_f(A/F_\infty)) = \text{rank}_{\mathcal{O}[[H]]}(X_f(B/F_\infty)).$$

Remark 4.1.2. Of course if we assume that $X(A/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -module, then $e_G(A) = \theta_{\mathcal{O}[[G]]}(X(A/F_\infty))$ by Lemma 2.3.1. It may still be of interest to prove the above theorem in general replacing $e_G(A)$ by $\theta_{\mathcal{O}[[G]]}(X(A/F_\infty))$. At present, we are not able to do this. The main difficulty in not being able to do this is that we do not have a good description of the pseudo-null $\mathcal{O}[[G]]$ -submodules of $X(A/F_\infty)(\pi)$ (if we do not assume that $X(A/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -module) and these modules may have subquotients which are not finitely generated over $k[[H]]$. For instance, the module $\mathcal{O}[[\Gamma]]/\pi^n$ is pseudo-null over $\mathcal{O}[[G]]$ but it has a subquotient $\mathcal{O}[[\Gamma]]/\pi$ which is not finitely generated over $k[[H]]$. But the same proposition tells us that the π -primary submodules will not cause a problem in our context once the power of the congruence is larger than the π -exponent.

In preparation of the proof, we first introduce the “mod π^n ” Selmer group which is a standard object to work with in the study of Selmer groups of congruent Galois representations (for instance, see [1, 4, 7, 13, 18, 19, 30, 32, 40, 41, 46]). Let $n \geq 1$. For every finite extension \mathcal{F} of F^{cyc} , we define $J_v(A[\pi^n]/\mathcal{F})$ to be

$$\bigoplus_{w|v} H^1(\mathcal{F}_w, A[\pi^n]) \text{ or } \bigoplus_{w|v} H^1(\mathcal{F}_w, A/A_v[\pi^n])$$

according as v does not or does divide p . We then define

$$J_v(A[\pi^n]/F_\infty) = \varinjlim_{\mathcal{F}} J_v(A[\pi^n]/\mathcal{F}),$$

where the direct limit is taken over all finite extensions \mathcal{F} of F^{cyc} contained in F_∞ . The mod π^n Selmer group is then defined by

$$S(A[\pi^n]/F_\infty) = \ker \left(H^1(G_S(F_\infty), A[\pi^n]) \longrightarrow \bigoplus_{v \in S} J_v(A[\pi^n]/F_\infty) \right).$$

We denote by $X(A[\pi^n]/F_\infty)$ the Pontryagin dual of $S(A[\pi^n]/F_\infty)$.

We introduce some more notation which will be needed in our discussion. Write $C_v = A$ for $v \nmid p$ and $C_v = A/A_v$ for $v|p$. For every prime w of F_∞ above v , we write $C_v(F_{\infty,w}) = (C_v)^{\text{Gal}(\bar{F}_v/F_{\infty,w})}$. We are now in the position to prove Theorem 4.1.1.

Proof of Theorem 4.1.1. Firstly, we note that if G_0 is an open normal subgroup of G and $H_0 = H \cap G_0$, then a finitely generated torsion $\mathcal{O}[[G]]$ -module satisfies $\mathfrak{M}_H(G)$ -property if and only if it satisfies $\mathfrak{M}_{H_0}(G_0)$ -property. Now by the theorem of Lazard (cf. [12, Cor. 8.34]), a compact p -adic Lie group always contains a open normal uniform pro- p subgroup. Hence to prove part (a) of the theorem, we may, and we will, assume that F_∞ is a strongly admissible pro- p p -adic Lie extension of F . In other words, G (and H) is pro- p without p -torsion. Write $e = e_G(A)$ and consider the following diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & S(A[\pi^{e+1}]/F_\infty) & \longrightarrow & H^1(G_S(F_\infty), A[\pi^{e+1}]) & \longrightarrow & \bigoplus_{v \in S} J_v(A[\pi^{e+1}]/F_\infty) \\ & & \downarrow & & \downarrow b & & \downarrow c \\ 0 & \longrightarrow & S(A/F_\infty)[\pi^{e+1}] & \longrightarrow & H^1(G_S(F_\infty), A)[\pi^{e+1}] & \longrightarrow & \bigoplus_{v \in S} J_v(A/F_\infty)[\pi^{e+1}] \end{array}$$

with exact rows. We write $c = \bigoplus_w c_w$, where w runs over the set of primes of F^{cyc} above S . Denote H_w to be the decomposition group of F_∞/F^{cyc} corresponding to a fixed prime of F_∞ , which we also denote by w , above w . Then we have $\ker c_w = \text{Coind}_H^{H_w}(C_v(F_{\infty,w})/\pi^{e+1})$, where v is the prime of F below w . This is clearly finitely generated over $\mathcal{O}[[H]]$ and is annihilated by π^{e+1} . On the other hand, the map b is easily seen to be surjective with $\ker b = A(F_\infty)/\pi^e$ being finite. Hence we have an exact sequence

$$0 \longrightarrow C \longrightarrow X(A/F_\infty)/\pi^{e+1} \longrightarrow X(A[\pi^{e+1}]/F_\infty) \longrightarrow D \longrightarrow 0$$

of $\mathcal{O}[[H]]$ -modules which are annihilated by $\pi^{\theta+1}$. Here C is a subquotient of the Pontryagin dual of $\ker c$ and D is a quotient of the Pontryagin dual of $\ker b$. In particular, C is a finitely generated $\mathcal{O}[[H]]$ -module

and D is finite. Therefore, we may apply Proposition 2.2.3 to conclude that $\frac{X(A[\pi^{e+1}]/F_\infty)}{X(A[\pi^{e+1}]/F_\infty)[\pi^e]}$ is finitely generated over $k[[H]]$ if and only if $\frac{X(A/F_\infty)/\pi^{e+1}}{(X(A/F_\infty)/\pi^{e+1})[\pi^e]}$ is finitely generated over $k[[H]]$. By Proposition 2.3.2, the latter is isomorphic to $X_f(A/F_\infty)/\pi$ and this module is in turn finitely generated over $k[[H]]$ as a consequence of the hypothesis that $X(A/F_\infty)$ satisfies $\mathfrak{M}_H(G)$ -property.

Now it follows from $(\mathbf{Cong}_{\mathbf{e}_G(\mathbf{A})+1})$ that there is an isomorphism

$$S(A[\pi^{e+1}]/F_\infty) \cong S(B[\pi^{e+1}]/F_\infty)$$

of $\mathcal{O}[[G]]$ -modules (and hence $\mathcal{O}[[H]]$ -modules) which in turn induces an isomorphism

$$\frac{X(A[\pi^{e+1}]/F_\infty)}{X(A[\pi^{e+1}]/F_\infty)[\pi^e]} \cong \frac{X(B[\pi^{e+1}]/F_\infty)}{X(B[\pi^{e+1}]/F_\infty)[\pi^e]}$$

of $k[[H]]$ -modules. Therefore, it follows that $\frac{X(B[\pi^{e+1}]/F_\infty)}{X(B[\pi^{e+1}]/F_\infty)[\pi^e]}$ is finitely generated over $k[[H]]$, and by Proposition 2.3.2, so is $X_f(B/F_\infty)/\pi$. It then follows from an application of Nakayama Lemma that $X_f(B/F_\infty)$ is finitely generated over $\mathcal{O}[[H]]$. This completes the proof of part (a) of the theorem.

We now prove (b). By assumption (ii) and the fact that $C_v(F_{\infty_w})/\pi^{e+1}$ is finite, we may apply Lemma 2.2.2 to conclude that $(\ker c)^\vee/(\ker c)^\vee[\pi^e]$ and $(\ker c)^\vee/\pi^e$ are finitely generated torsion $k[[H]]$ -modules. By Lemma 2.2.4, this in turn implies that $C/C[\pi^e]$ and C/π^e are finitely generated torsion $k[[H]]$ -modules. Therefore, it follows from Propositions 2.2.3 and 2.3.2 that

$$\mathrm{rank}_{k[[H]]} \left(X_f(A/F_\infty)/\pi \right) = \mathrm{rank}_{k[[H]]} \left(\frac{X(A[\pi^{e+1}]/F_\infty)}{X(A[\pi^{e+1}]/F_\infty)[\pi^e]} \right) = \mathrm{rank}_{k[[H]]} \left(\frac{X(B[\pi^{e+1}]/F_\infty)}{X(B[\pi^{e+1}]/F_\infty)[\pi^e]} \right).$$

Here the second equality follows from the above isomorphism deduced from the $(\mathbf{Cong}_{\mathbf{e}_G(\mathbf{A})+1})$ condition. By a similar argument as above, we obtain an exact sequence

$$0 \longrightarrow C' \longrightarrow X(B/F_\infty)/\pi^{e+1} \longrightarrow X(B[\pi^{e+1}]/F_\infty) \longrightarrow D' \longrightarrow 0$$

of $\mathcal{O}[[H]]$ -modules which are annihilated by π^{e+1} , where $C'/C'[\pi^e]$ and C'/π^e are finitely generated torsion $k[[H]]$ -modules, and D' is finite. By Proposition 2.2.3, we then have

$$\mathrm{rank}_{k[[H]]} \left(X_f(A/F_\infty)/\pi \right) = \mathrm{rank}_{k[[H]]} \left(\frac{X(B[\pi^{e+1}]/F_\infty)}{X(B[\pi^{e+1}]/F_\infty)[\pi^e]} \right) = \mathrm{rank}_{k[[H]]} \left(\frac{X(B/F_\infty)/\pi^{e+1}}{(X(B/F_\infty)/\pi^{e+1})[\pi^e]} \right).$$

But the last quantity is precisely $\mathrm{rank}_{k[[H]]} \left(X_f(B/F_\infty)/\pi \right)$ by Proposition 2.3.3. The required equality now follows an application of [22, Corollary 1.10] (or [31, Proposition 4.12]) and the fact that the π -free quotients of the dual Selmer groups have no π -torsion. \square

4.2 Comparing characteristic elements of Selmer groups

In this subsection, we will prove our main results concerning with the characteristic elements of the Selmer groups. In preparation of this, we need to recall some further notion and notation from [8]. Let

$$\Sigma = \{ s \in \mathcal{O}[[G]] \mid \mathcal{O}[[G]]/\mathcal{O}[[G]]s \text{ is a finitely generated } \mathcal{O}[[H]]\text{-module} \}.$$

By [8, Theorem 2.4], Σ is a left and right Ore set consisting of non-zero divisors in $\mathcal{O}[[G]]$. Set $\Sigma^* = \cup_{n \geq 0} \pi^n \Sigma$. It follows from [8, Proposition 2.3] that a finitely generated $\mathcal{O}[[G]]$ -module M is annihilated by Σ^* if and only if M satisfies the $\mathfrak{M}_H(G)$ -property. By abuse of notion, we shall denote $\mathfrak{M}_H(G)$ to be the category of all finitely generated $\mathcal{O}[[G]]$ -modules which are Σ^* -torsion. It follows from the discussion in [8, Section 3] that we have the following exact sequence

$$K_1(\mathcal{O}[[G]]) \longrightarrow K_1(\mathcal{O}[[G]]_{\Sigma^*}) \xrightarrow{\partial_G} K_0(\mathfrak{M}_H(G)) \longrightarrow 0$$

of K -groups. For each M in $\mathfrak{M}_H(G)$, we define a *characteristic element* for M to be any element ξ_M in $K_1(\mathbb{Z}_p[[G]]_{\Sigma^*})$ which has the property that

$$\partial_G(\xi_M) = -[M].$$

Let $\rho : G \longrightarrow GL_m(\mathcal{O}_\rho)$ denote a continuous group representation, where $\mathcal{O}' = \mathcal{O}_\rho$ is the ring of integers of some finite extension of K . For $g \in G$, we write \bar{g} for its image in $\Gamma = G/H$. We define a continuous group homomorphism

$$G \longrightarrow M_d(\mathcal{O}') \otimes_{\mathcal{O}} \mathcal{O}[[\Gamma]], \quad g \mapsto \rho(g) \otimes \bar{g}.$$

By [8, Lemma 3.3], this in turn induces a map

$$\Phi_\rho : K_1(\mathcal{O}[[G]]_{\Sigma^*}) \longrightarrow Q_{\mathcal{O}'}(\Gamma)^\times,$$

where $Q_{\mathcal{O}'}(\Gamma)$ is the field of fraction of $\mathcal{O}'[[\Gamma]]$. Let $\varphi : \mathcal{O}'[[\Gamma]] \longrightarrow \mathcal{O}'$ be the augmentation map and denote its kernel by \mathfrak{p} . One can extend φ to a map $\varphi : \mathcal{O}'[[\Gamma]]_{\mathfrak{p}} \longrightarrow K'$, where K' is the field of fraction of \mathcal{O}' . Let ξ be an arbitrary element in $K_1(\mathcal{O}[[G]]_{\Sigma^*})$. If $\Phi_\rho(\xi) \in \mathcal{O}'[[\Gamma]]_{\mathfrak{p}}$, we define $\xi(\rho)$ to be $\varphi(\Phi_\rho(\xi))$. If $\Phi_\rho(\xi) \notin \mathcal{O}'[[\Gamma]]_{\mathfrak{p}}$, we set $\xi(\rho)$ to be ∞ .

Suppose for now G (and hence H) has no p -torsion. Following [9], we say that the *Akashi series* of M exists if $H_i(H, M)$ is $\mathcal{O}[[\Gamma]]$ -torsion for every i . In the case of this event, we denote $Ak_H(M)$ to be the *Akashi series* of M which is defined to be

$$\prod_{i \geq 0} g_i^{(-1)^i},$$

where g_i is the characteristic polynomial of $H_i(H, M)$. Of course, the Akashi series is only well-defined up to a unit in $\mathcal{O}[[\Gamma]]$. Also, note that since G (and hence H) has no p -torsion, H has finite p -cohomological dimension (cf. [39, Corollaire 1]), and therefore, the alternating product is a finite product. We can now state the following result which answer [8, Conjecture 4.8 Case 4] partially, and is proven in [29, Proposition 6.2] and [30, Proposition 6.2].

Proposition 4.2.1. *Let $M \in \mathfrak{M}_H(G)$. Suppose that M contains no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules. Let ξ_M be a characteristic element of M . Then the following statements are equivalent.*

- (a) $\xi_M \in \alpha(\mathcal{O}[[G]]^\times)$, where α is the map $\mathcal{O}[[G]]_{\Sigma^*}^\times \longrightarrow K_1(\mathcal{O}[[G]]_{\Sigma^*})$.

- (b) $\xi_M(\rho)$ is finite and lies in \mathcal{O}_ρ^\times for every continuous group representation ρ of G .
- (c) $\Phi_\rho(\xi_M) \in \mathcal{O}_\rho[[\Gamma]]^\times$ for every continuous group representation ρ of G .
- (d) $\Phi_\rho(\xi_M) \in \mathcal{O}_\rho[[\Gamma]]^\times$ for every Artin representation ρ of G .
- (e) There exists an open normal pro- p subgroup G' of G such $Ak_{H'}(X(A/F_\infty)) \in \mathcal{O}[[\Gamma']]^\times$. Here $H' = H \cap G'$ and $\Gamma' = G'/H'$.

Remark 4.2.2. By [8, Lemma 4.9], the implications $(a) \Rightarrow (b) \Leftrightarrow (c) \Rightarrow (d)$ always hold without the pseudo-nullity assumption on M . By examining the proof of [30, Proposition 6.2] (or rather [30, Proposition 6.1]), we see that the implication $(d) \Rightarrow (e)$ also holds without the pseudo-nullity assumption. It is the implication $(e) \Rightarrow (a)$, where the pseudo-nullity assumption is required.

We can now state and prove the following theorem which slightly refines [30, Theorem 6.3]. If $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property, we denote by $\xi_{A,f}$ a characteristic element of $X_f(A/F_\infty)$. Now if $X(B/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property, then $\xi_{B,f}$ is defined similarly. We continue to write α_G for the natural map

$$\mathcal{O}[[G]]_{\Sigma^*}^\times \longrightarrow K_1(\mathcal{O}[[G]]_{\Sigma^*}).$$

Theorem 4.2.3. *Let F_∞ be a strongly admissible p -adic Lie extension of F . Suppose that the following conditions are satisfied.*

- (a) *The condition $(\mathbf{Cong}_{\theta_G(\mathbf{A})+1})$ is satisfied.*
- (b) *$X(A/F_\infty)$ (and hence $X(B/F_\infty)$) satisfies the $\mathfrak{M}_H(G)$ -property.*
- (c) *$X(B/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules.*
- (d) *For every $v \in S$, the decomposition group of G at v has dimension ≥ 2 .*

Then if $\xi_{A,f} \in \alpha_G(\mathcal{O}[[G]]^\times)$, so is $\xi_{B,f}$.

Proof. Suppose that $\xi_{A,f} \in \alpha_G(\mathcal{O}[[G]]^\times)$. Then by Proposition 4.2.1 and the remark thereafter, there exists an open normal pro- p subgroup G' of G such $Ak_{H'}(X_f(A/F_\infty)) \in \mathcal{O}[[\Gamma']]^\times$, where $H' = H \cap G'$. By [29, Proposition 5.4] or [30, Proposition 2.2], this in turn implies that $X_f(A/F_\infty)$ is a finitely generated torsion $\mathcal{O}[[H']]$ -module. By virtue of assumption (d) and Theorem 4.1.1, it follows that $X_f(B/F_\infty)$ is a finitely generated torsion $\mathcal{O}[[H']]$ -module. By a well-known theorem of Venjakob (cf. [45, Example 2.3 and Proposition 5.4]), this in turn implies that $X_f(B/F_\infty)$ is a finitely generated pseudo-null $\mathcal{O}[[G']]$ -module. On the other hand, it follows from assumption (c) and [43, Lemma 4.2] that $X_f(B/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules. Consequently, we have $X_f(B/F_\infty) = 0$, or $\partial_G(\xi_{B,f}) = 0$. It then follows from the above exact sequence of K -groups that there exists an element in $K_1(\mathcal{O}[[G]])$ which maps to $\xi_{B,f}$. On the other hand, it is well-known that $\mathcal{O}[[G]]^\times$ maps onto $K_1(\mathcal{O}[[G]])$, and the required conclusion is now immediate from this. \square

We end the subsection recording the following result for completeness. Write $\xi_{A,\pi}$ (resp., $\xi_{B,\pi}$) for a characteristic element of $X(A/F_\infty)(\pi)$ (resp., a characteristic element of $X_f(B/F_\infty)(\pi)$). Note that π -primary modules automatically satisfy $\mathfrak{M}_H(G)$ -property, and hence one can always attach characteristic elements to them.

Theorem 4.2.4. *Let F_∞ be a strongly admissible p -adic Lie extension of F . Suppose that the following conditions are satisfied.*

- (a) *The condition **(Cong₁)** is satisfied.*
- (b) *$X(A/F_\infty)$ is a torsion $\mathcal{O}[[G]]$ -module.*
- (c) *$\xi_{A,\pi} \in \alpha_G(\mathcal{O}[[G]]^\times)$.*

Then $X(B/F_\infty)$ is a torsion $\mathcal{O}[[G]]$ -module and $\xi_{B,\pi} \in \alpha_G(\mathcal{O}[[G]]^\times)$.

Proof. By Proposition 4.2.1 and the remark thereafter, there exists an open normal pro- p subgroup G' of G such $Ak_{H'}(X(A/F_\infty)(\pi)) \in \mathcal{O}[[G']]^\times$, where $H' = H \cap G'$. On the other hand, it is not difficult to deduce from the definition of the Akashi series and [29, Lemma 2.2] that

$$Ak_{H'}(X(A/F_\infty)(\pi)) = \pi^{\mu_{\mathcal{O}[[G']]}(X(A/F_\infty))}.$$

Hence we conclude that

$$\mu_{\mathcal{O}[[G']]}(X(A/F_\infty)) = 0.$$

By [32, Theorem 4.2.1], this in turn implies that $X(B/F_\infty)$ is a torsion $\mathcal{O}[[G]]$ -module and

$$\mu_{\mathcal{O}[[G']]}(X(B/F_\infty)) = 0.$$

By [6, Definition 4.1], $-1 \in K_1(\mathcal{O}[[G']]_\Sigma)$ is a characteristic element for $X(B/F_\infty)(\pi)$. Since $\mathcal{O}[[G]]^\times$ maps onto $K_1(\mathcal{O}[[G]])$, we have that every characteristic element for $X(B/F_\infty)(\pi)$ lies in $\alpha_{G'}(\mathcal{O}[[G']]^\times)$. It then follows from this and [3, Theorem 6.8] that $\xi_{B,\pi} \in \alpha_G(\mathcal{O}[[G]]^\times)$ which is what we want to show. \square

4.3 Comparing specializations of a big Galois representation

We now apply the main result in Subsection 4.1 to compare the Selmer groups of specializations of a big Galois representation. As before, let p be a prime. We let F be a number field. If $p = 2$, we assume further that F has no real primes. Denote \mathcal{O} to be the ring of integers of some finite extension K of \mathbb{Q}_p . We write $R = \mathcal{O}[[T]]$ for the power series ring in one variable. Suppose that we are given the following set of data:

- (a) \mathcal{A} is a cofree R -module of R -corank d with a continuous, R -linear $\text{Gal}(\bar{F}/F)$ -action which is unramified outside a finite set of primes of F .
- (b) For each prime v of F above p , \mathcal{A}_v is a $\text{Gal}(\bar{F}_v/F_v)$ -submodule of \mathcal{A} which is cofree of R -corank d_v .

(c) For each real prime v of F , we write $\mathcal{A}_v^+ = \mathcal{A}^{\text{Gal}(\bar{F}_v/F_v)}$ which we assume to be cofree of R -corank d_v^+ .

(d) The quantities d, d_v and d_v^+ satisfy the following identity

$$\sum_{v|p} (d - d_v)[F_v : \mathbb{Q}_p] = dr_2(F) + \sum_{v \text{ real}} (d - d_v^+), \quad (2)$$

where $r_2(F)$ is the number of complex primes of F .

For any prime element f of $\mathcal{O}[[T]]$ such that $\mathcal{O}[[T]]/f$ is a maximal order, then we can obtain a datum $(\mathcal{A}[f], \{\mathcal{A}_v[f]\}_{v|p}, \{\mathcal{A}_v^+[f]\}_{v|\mathbb{R}})$ in the sense of Section 3. The next lemma has a easy proof which is left to reader.

Lemma 4.3.1. *Let f and g be prime elements of $\mathcal{O}[[T]]$ with $\pi^n|(f - g)$ such that $\mathcal{O}[[T]]/f$ and $\mathcal{O}[[T]]/g$ are maximal orders. Then $\mathcal{A}[f, \pi^n] = \mathcal{A}[g, \pi^n]$. One also has similar conclusions for \mathcal{A}_v and \mathcal{A}_v^+ .*

The next proposition compares the π -free quotient of the dual Selmer groups of various specializations of a big Galois representation. For a real number x , we denote $[x]$ to be the smallest integer not less than x . We can now state and prove the following theorem which is a refinement of [41, Proposition 8.6], [5, Corollary 4.37] and [32, Proposition 5.2.3].

Theorem 4.3.2. *Let F_∞ be an admissible p -adic Lie extension of F . Let f be a prime element of $\mathcal{O}[[T]]$ such that $\mathcal{O}' := \mathcal{O}[[T]]/f$ is a maximal order. Set $A = \mathcal{A}[f]$ and suppose that $X(A/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property. Set*

$$n := \left\lceil \frac{e_{\mathcal{O}'[[G]]}(X(A/F_\infty)) + 1}{m} \right\rceil,$$

where m is the ramification index of \mathcal{O}'/\mathcal{O} . Suppose that g is a prime element of $\mathcal{O}[[T]]$ with $\pi^n|f - g$ such that $\mathcal{O}[[T]]/g$ is isomorphic to \mathcal{O}' and $X(\mathcal{A}[g]/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodule. Then we have that $X(\mathcal{A}[g]/F_\infty)$ satisfies the $\mathfrak{M}_H(G)$ -property.

Suppose further that the following statements hold.

(i) F_∞ is a strongly S -admissible pro- p p -adic Lie extension of F .

(ii) For every $v \in S$, the decomposition group of G at v has dimension ≥ 2 .

Then we also have

$$\text{rank}_{\mathcal{O}'[[H]]}(X_f(A/F_\infty)) = \text{rank}_{\mathcal{O}'[[H]]}(X_f(\mathcal{A}[g]/F_\infty)).$$

Proof. Let g be a prime element of $\mathcal{O}[[T]]$ which satisfies the hypothesis in the theorem. Let π' be a prime element of \mathcal{O}' and write $B = \mathcal{A}[g]$. It follows from Lemma 4.3.1 that there is an isomorphism of $G_S(F)$ -modules $A[\pi'^{mn}] \cong B[\pi'^{mn}]$ which induces an isomorphism of $\text{Gal}(\bar{F}_v/F_v)$ -modules $A_v[\pi'^{mn}] \cong B_v[\pi'^{mn}]$ for each prime v of F above p . By our hypothesis of n , we have $mn \geq e_{\mathcal{O}'[[G]]}(A) + 1$. In particular, the congruence hypothesis $(\mathbf{C}_{e_{\mathcal{O}'[[G]]}(A)+1})$ holds for A and $\mathcal{A}[g]$. Hence the conclusion of the theorem is now immediate from an application of Theorem 4.1.1. \square

Remark 4.3.3. As noted in the Introduction, the above equality of $\mathcal{O}[[H]]$ -ranks supports the prediction in [41, Theorem 8.8]. The proof in [41, Theorem 8.8] rests on the (presumably) much stronger assumption that the Selmer group of the big Galois representation satisfies the $\mathfrak{M}_H(G)$ -property. However, at our current state of knowledge, it is not even clear if this latter assumption is a consequence of the assumption that the Selmer group of every specialization satisfies the $\mathfrak{M}_H(G)$ -property (but see [11, Proposition 5.4] and [41, Proposition 8.6] for discussion in this direction). Finally, we mention that it would be interesting to prove such an equality for specializations which are congruent by a power smaller than the π -exponent of the dual Selmer group under the hypothesis of Theorem 4.3.2. At present, we do not know how to prove this equality, even with the added assumption that the Selmer group of every specialization satisfies the $\mathfrak{M}_H(G)$ -property. The point is that our methods here do not seem to be able to compare the Selmer groups when the congruence is smaller than the π -exponent. Note that the method of [41, Theorem 8.8] breaks down here too, as we do not know whether the Selmer group of the big Galois representation satisfies the $\mathfrak{M}_H(G)$ -property, and so we cannot compare the $\mathcal{O}[[H]]$ -rank of the π -free quotient of the dual Selmer groups of the specialization with the R -free quotient of the $R[[H]]$ -rank of the dual Selmer group of the big Galois representation.

A Nonexistence of pseudo-null submodules

As our main result (Theorem 4.1.1) requires that our Selmer groups to have no nonzero pseudo-null submodules, we shall briefly discuss this property here. Namely, we give a sufficient criterion of this property. As before, let p be a prime and F a number field. **If $p = 2$, assume further that F has no real primes.** Let $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$ be a datum which satisfy the conditions (a)-(d) as in Section 3. Denote by S a finite set of primes of F which contains all the primes above p , the ramified primes of A and the archimedean primes. *We will also assume that the data obtained by base change over every finite extension of L of F in F_∞ also satisfy the conditions (a)-(d).* Note that this assumption is automatically satisfied when F_∞ is a pro- p extension of F by Lemma 3.1.1 (and noting our standing assumption that if $p = 2$, then F has no real primes). We can now state the main result of this appendix.

Proposition A.1. *Let F_∞ be a strongly admissible p -adic Lie extension of F . Suppose that the following statements are valid.*

- (i) $X(A/F_\infty)$ is a torsion $\mathcal{O}[[G]]$ -module.
- (ii) *For every $v \in S$, the decomposition group of G at v has dimension ≥ 2 , and for those v above p , the decomposition group of G at v has dimension ≥ 3 .*

Then $X(A/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules.

We should mention that the first proof of such results in the noncommutative situation goes back to the work of Ochi and Venjakob [35]. Later, in [20], Hachimori and Ochiai gave a proof which simplified part of the original argument in [35], and it is this latter approach we adopt here.

To prepare for the proof of the proposition, we recall the (Tate) dual data of $(A, \{A_v\}_{v|p}, \{A_v^+\}_{v|\mathbb{R}})$. For a \mathcal{O} -module N , we denote $T_\pi(N)$ to be its π -adic Tate module, i.e., $T_\pi(N) = \varprojlim_i N[\pi^i]$. We then set $A^* = \text{Hom}_{\text{cts}}(T_\pi(A), \mu_{p^\infty})$. Similarly, for each $v|p$ (resp., v real), we set $A_v^* = \text{Hom}_{\text{cts}}(T_\pi(A/A_v), \mu_{p^\infty})$ (resp., $(A^*)_v^+ = \text{Hom}_{\text{cts}}(T_\pi(A/A_v^+), \mu_{p^\infty})$). It is an easy exercise to verify that $(A^*, \{A_v^*\}_{v|p}, \{(A^*)_v^+\}_{v|\mathbb{R}})$ satisfies equality (2). The Selmer group attached to this dual data is denoted by $S(A^*/F_\infty)$, whose Pontryagin dual is denoted to be $X(A^*/F_\infty)$.

Lemma A.2. *Retain the assumptions in Proposition A.1. Then we have $H^2(G_S(F_\infty), A) = 0$ and a short exact sequence*

$$0 \longrightarrow S(A/F_\infty) \longrightarrow H^1(G_S(F_\infty), A) \longrightarrow \bigoplus_{v \in S} J_v(A/F_\infty) \longrightarrow 0.$$

Proof. Since $X(A/F_\infty)$ is a torsion $\mathcal{O}[[G]]$ -module, it follows from [32, Corollary 4.1.2] that $X(A^*/F_\infty)$ is also a torsion $\mathcal{O}[[G]]$ -module. Recall that the fine Selmer group of A^* (in the sense of [10]; see also [31]) is defined by the following exact sequence

$$0 \longrightarrow R(A^*/F_\infty) \longrightarrow H^1(G_S(F_\infty), A^*) \longrightarrow \bigoplus_{v \in S} K_v(A^*/F_\infty),$$

Here $K_v^i(A^*/F_\infty) = \varinjlim_L \bigoplus_{w|v} H^i(L_w, A^*)$, where the direct limit is taken over all finite extensions L of F contained in F_∞ under the restriction maps. We write $Y(A^*/F_\infty)$ for the Pontryagin dual of $R(A^*/F_\infty)$. Clearly, we have an injection $R(A^*/F_\infty) \hookrightarrow S(A^*/F_\infty)$ which in turn induces a surjection $X(A^*/F_\infty) \twoheadrightarrow Y(A^*/F_\infty)$. Since $X(A^*/F_\infty)$ is torsion over $\mathcal{O}[[G]]$, so is $Y(A^*/F_\infty)$. It then follows from [31, Lemma 7.1] that $H^2(G_S(F_\infty), A) = 0$ and this proves the first assertion of the lemma.

Now combining the Poitou-Tate sequence with the assertion of $H^2(G_S(F_\infty), A) = 0$, we obtain an exact sequence

$$0 \longrightarrow S(A/F_\infty) \longrightarrow H^1(G_S(F_\infty), A) \longrightarrow \bigoplus_{v \in S} J_v(A/F_\infty) \longrightarrow (\widehat{S}(A^*/F_\infty))^\vee \longrightarrow 0$$

and an injection

$$\varprojlim_L H^1(G_S(L), T_\pi A^*) \longrightarrow \varprojlim_L \bigoplus_{w \in S_L} H^1(L_w, T_\pi A^*),$$

Here $\widehat{S}(A^*/F_\infty)$ is defined as the kernel of the map

$$\varprojlim_L H^1(G_S(L), T_\pi A^*) \longrightarrow \varprojlim_L \bigoplus_{w \in S_L} T_\pi H^1(L_w, A^*),$$

where the inverse limit is taken over all finite extensions L of F contained in F_∞ . By [35, Lemma 5.4], $\varprojlim_L \bigoplus_{w \in S_L} H^1(L_w, T_\pi A^*)$ is a torsionfree $\mathcal{O}[[G]]$ -module. It then follow from this and the above injection that $\widehat{S}(A^*/F_\infty)^\vee$ is also a torsionfree $\mathcal{O}[[G]]$ -module. On the other hand, taking the torsionness of $X(A/F_\infty)$, the vanishing of $H^2(G_S(F_\infty), A)$, property (d) of our datum and the formulas in [36, Theorem 4.1] and [21,

Theorem 7.1] into account, followed by a straightforward rank calculation, we have that $\widehat{S}(A^*/F_\infty)^\vee$ has zero $\mathcal{O}[[G]]$ -rank. Hence this forces $\widehat{S}(A^*/F_\infty) = 0$ and the required short exact sequence is a consequence of this. \square

We finally finish with the proof of the main result of this appendix.

Proof of Proposition A.1. By Lemma A.2, we have a short exact sequence

$$0 \longrightarrow \left(\bigoplus_{v \in S} J_v(A/F_\infty) \right)^\vee \longrightarrow H^1(G_S(F_\infty), A)^\vee \longrightarrow X(A/F_\infty) \longrightarrow 0.$$

The leftmost module in the sequence is a reflexive $\mathcal{O}[[G]]$ -module by [35, Lemma 5.4]. Since $H^2(G_S(F_\infty), A) = 0$ by Lemma A.2, it follows from an application of [35, Theorem 4.7] that $H^1(G_S(F_\infty), A)^\vee$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules. We may therefore now apply [20, Proposition 3.5] to conclude that $X(A/F_\infty)$ has no nonzero pseudo-null $\mathcal{O}[[G]]$ -submodules. \square

References

- [1] S. Ahmed and S. Shekhar, λ -invariants of Selmer groups of elliptic curves with positive μ -invariant, *J. Ramanujan Math. Soc.* 30(1) (2015) 115–133.
- [2] K. Ardakov and K. A. Brown, Primeness, semiprimeness and localisation in Iwasawa algebras, *Trans. Amer. Math. Soc.* 359(4) (2007) 1499–1515.
- [3] K. Ardakov and S. Wadsley, Characteristic elements for p -torsion Iwasawa modules, *J. Algebraic Geom.* 15 (2006) 339–377.
- [4] R. Barman and A. Saikia, A note on Iwasawa μ -invariants of elliptic curves, *Bull. Braz. Math. Soc., New Series* 41(3) (2010) 399–407.
- [5] P. Barth, Iwasawa theory for one-parameter families of motives, *Int. J. Number Theory* 9(2) (2013) 257–319.
- [6] D. Burns and O. Venjakob, On descent theory and main conjectures in non-commutative Iwasawa theory, *J. Inst. Math. Jussieu* 10(1) (2011) 59–118.
- [7] A. Chandrakant Sharma, Iwasawa invariants for the False-Tate extension and congruences between modular forms, *J. Number Theory* 129 (2009) 1893–1911.
- [8] J. Coates, T. Fukaya, K. Kato, R. Sujatha and O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication, *Publ. Math. IHES* 101 (2005) 163–208.
- [9] J. Coates, P. Schneider and R. Sujatha, Links between cyclotomic and GL_2 Iwasawa theory. Kazuya Kato’s fiftieth birthday. *Doc. Math.* 2003, Extra Vol., 187–215 (electronic).
- [10] J. Coates and R. Sujatha, Fine Selmer groups of elliptic curves over p -adic Lie extensions, *Math. Ann.* 331(4) (2005) 809–839.
- [11] ———, On the $\mathfrak{M}_H(G)$ -conjecture. *Non-abelian fundamental groups and Iwasawa theory*, 132–161, London Math. Soc. Lecture Note Ser., 393, Cambridge Univ. Press, Cambridge, 2012.
- [12] J. Dixon, M. P. F. Du Sautoy, A. Mann and D. Segal, *Analytic Pro- p Groups*, 2nd edn, Cambridge Stud. Adv. Math. 38, Cambridge Univ. Press, Cambridge, UK, 1999.
- [13] M. Emerton, R. Pollack and T. Weston, Variation of Iwasawa invariants in Hida families, *Invent. Math.* 163 (2006) 523–580.

- [14] T. Fukaya and K. Kato, A formulation of conjectures on p -adic zeta functions in noncommutative Iwasawa theory, *Proceedings of the St. Petersburg Mathematical Society. Vol. XII*, 1–85, Amer. Math. Soc. Transl. Ser. 2 219, Amer. Math. Soc., Providence, RI, 2006.
- [15] K. R. Goodearl and R. B. Warfield, *An introduction to non-commutative Noetherian rings*, London Math. Soc. Stud. Texts 61, Cambridge University Press, 2004.
- [16] R. Greenberg, Iwasawa theory for p -adic representations, in *Algebraic Number Theory—in honor of K. Iwasawa*, ed. J. Coates, R. Greenberg, B. Mazur and I. Satake, Adv. Std. in Pure Math. 17, 1989, pp. 97–137.
- [17] ———, Iwasawa theory for p -adic deformations of motives, *Proc. Sympos. Pure Math.* 55 (Part 2) (1994) 193–223.
- [18] R. Greenberg and V. Vatsal, On the Iwasawa invariants of elliptic curves, *Invent. Math.* 142 (2000) 17–63.
- [19] Y. Hachimori, Iwasawa λ -invariants and congruence of Galois representations, *J. Ramanujan Math. Soc.* 26(2) (2011) 203–217.
- [20] Y. Hachimori and T. Ochiai, Notes on non-commutative Iwasawa theory, *Asian J. Math.* 14(1) (2010) 11–17.
- [21] Y. Hachimori and O. Venjakob, Completely faithful Selmer groups over Kummer extensions, *Doc. Math.* 2003 (2003) 443–478, Extra Volume: Kazuya Kato’s fiftieth birthday.
- [22] S. Howson, Euler characteristic as invariants of Iwasawa modules, *Proc. London Math. Soc.* 85(3) (2002) 634–658.
- [23] ———, Structure of central torsion Iwasawa modules, *Bull. Soc. Math. France* 130(4) (2002) 507–535.
- [24] S. Jha, Fine Selmer group of Hida deformations over non-commutative p -adic Lie extensions, *Asian J. Math.* 16(2) (2012) 353–366.
- [25] M. Kakde, The main conjecture of Iwasawa theory for totally real fields, *Invent. Math.* 193(3) (2013) 539–626.
- [26] K. Kato, p -adic Hodge theory and values of zeta functions of modular forms, in: *Cohomologies p -adiques et applications arithmétiques. III.*, Astérisque 295, 2004, ix, 117–290.
- [27] T. Y. Lam, *Lectures on Modules and Rings*, Grad. Texts in Math. 189, Springer, 1999.
- [28] M. Lazard, Groups analytiques p -adiques, *Publ. Math. IHES* 26 (1965) 389–603.
- [29] M. F. Lim, A remark on the $\mathfrak{M}_H(G)$ -conjecture and Akashi series, *Int. J. Number Theory* 11(1) (2015) 269–297.
- [30] ———, Akashi series, characteristic elements and congruence of Galois representations, *Int. J. Number Theory* 12(3) (2016) 593–613.
- [31] ———, Notes on the fine Selmer groups, accepted for publication in *Asian J. Math*, also available at [arXiv:1306.2047 \[math.NT\]](#).
- [32] ———, Comparing the π -primary submodules of the dual Selmer groups, available at [arXiv:1409.0942v2 \[math.NT\]](#).
- [33] J. Nekovář, *Selmer Complexes*, Astérisque 310, 2006.
- [34] A. Neumann, Completed group algebras without zero divisors, *Arch. Math.* 51(6) (1988) 496–499.
- [35] Y. Ochi and O. Venjakob, On the structure of Selmer groups over p -adic Lie extensions, *J. Algebraic Geom.* 11(3) (2002) 547–580.
- [36] ———, On the ranks of Iwasawa modules over p -adic Lie extensions, *Math. Proc. Cambridge Philos. Soc.* 135 (2003), no. 1, 25–43.
- [37] T. Ochiai, On the two-variable Iwasawa main conjecture, *Comp. Math.* 142 (2006) 1157–1200.
- [38] L. Ribes and P. Zalesskii, *Profinite Groups*, Second edition, Ergeb. Math. Grenzgeb. 40, Springer, 2010.
- [39] J.-P. Serre, Sur la dimension cohomologique des groupes profinis, *Topology* 3 (1965) 413–420.
- [40] S. Shekhar, Euler characteristics of Λ -adic forms over Kummer extensions, *Int. J. Number Theory* 10(2) (2014) 401–420.

- [41] S. Shekhar and R. Sujatha, On the structure of Selmer groups of Λ -adic deformations over p -adic Lie extensions, *Doc. Math.* 17 (2012) 573–606.
- [42] _____, Euler characteristic and congruences of elliptic curves, *Münster J. of Math.* 7 (2014) 327–343.
- [43] R. Sujatha, Iwasawa theory and modular forms, *Pure Appl. Math. Q.* 2(2) (2006) 519–538.
- [44] O. Venjakob, On the structure theory of the Iwasawa algebra of a p -adic Lie group, *J. Eur. Math. Soc.* 4(3) (2002) 271–311.
- [45] _____, A non-commutative Weierstrass preparation theorem and applications to Iwasawa theory, *J. reine angew. Math.* 559 (2003) 153–191.
- [46] T. Weston, Iwasawa invariants of Galois deformations, *Manuscripta Math.* 118(2) (2005) 161–180.
- [47] J. Wilson, *Profinite Groups*, London Math. Soc. Monogr. Ser. 19, The Clarendon Press, Oxford University Press, 1998.